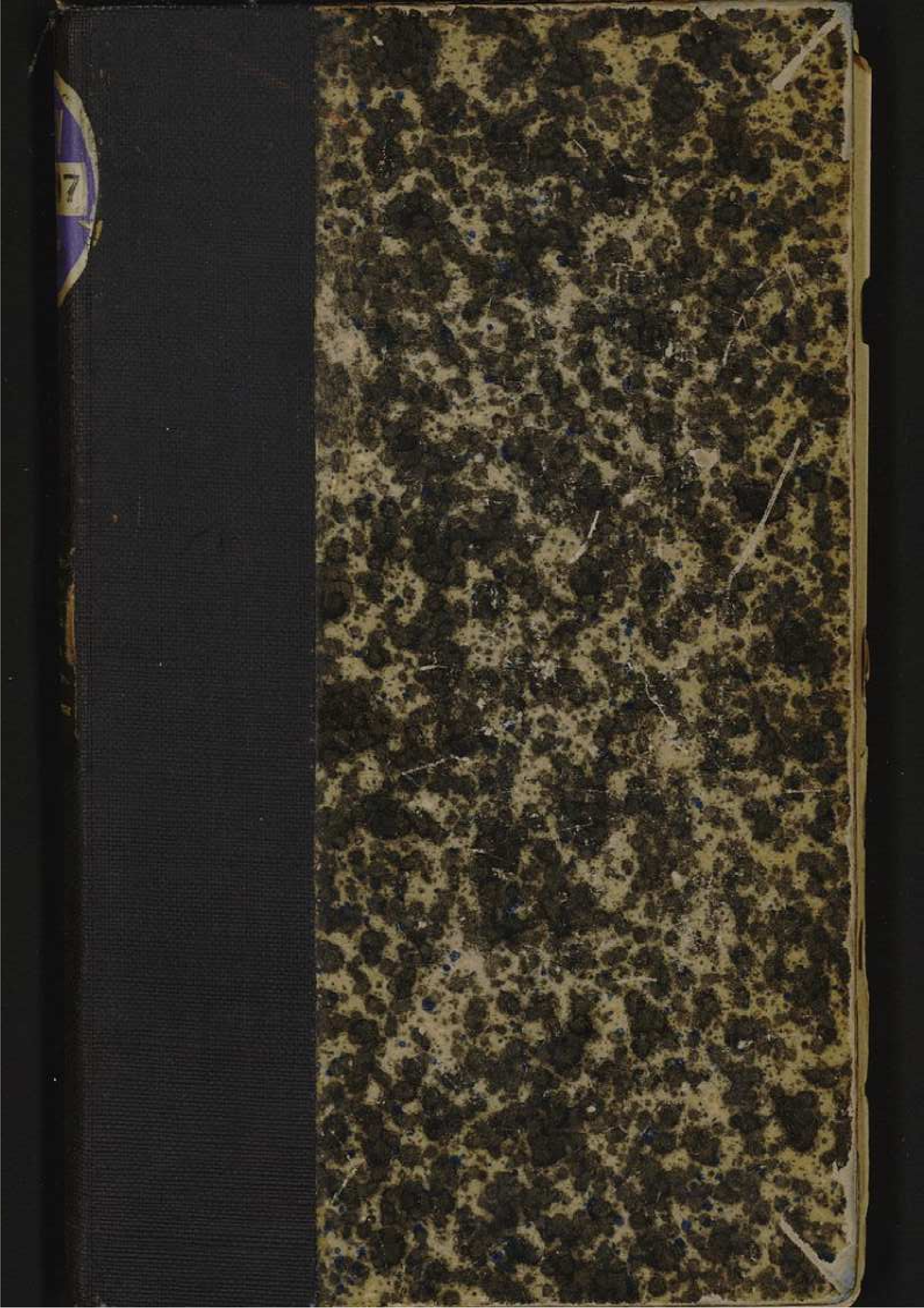
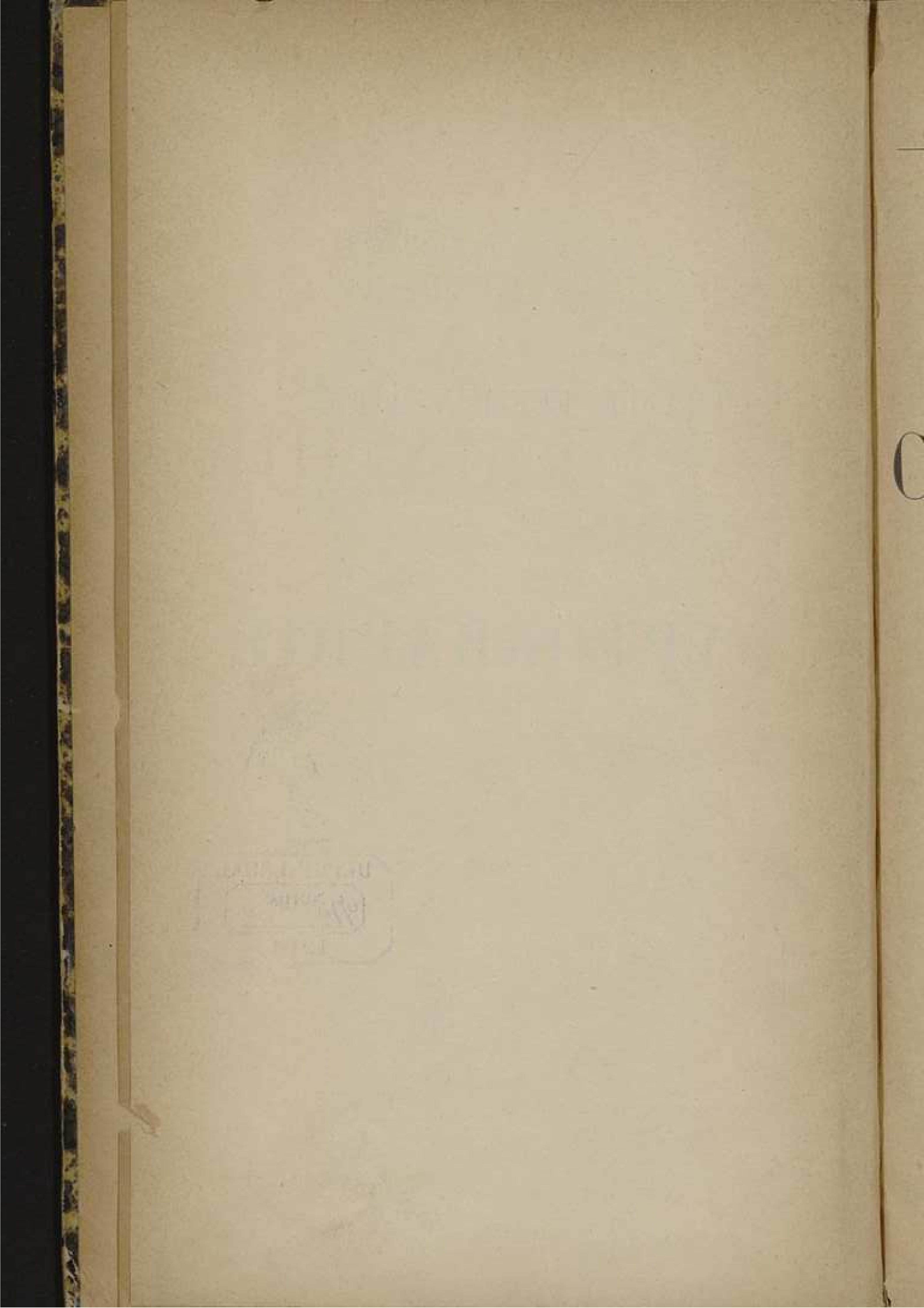

17

TRAITÉ ÉLÉMENTAIRE

DE

CRYPTOGRAPHIE



MATHÉMATIQUES APPLIQUÉES

TRAITÉ ÉLÉMENTAIRE

DE

CRYPTOGRAPHIE

PAR

F. DELASTELLE

Prix : 5 francs

PARIS

GAUTHIER-VILLARS, IMPRIMEUR-LIBRAIRE

DE L'ÉCOLE POLYTECHNIQUE, DU BUREAU DES LONGITUDES

Quai des Grands-Augustins, 55.

1902

AVANT-PROPOS

Rien de plus étrange que les idées qui ont généralement cours sur la cryptographie.

Sans parler des personnes, plus nombreuses qu'on ne pense, qui croient pouvoir correspondre secrètement sans conventions préalables, non plus que de celles qui s'imaginent que leur secret sera assuré si elles changent seulement la forme des lettres ou les permutent entre elles, combien de cryptographes recourent à des complications, souvent inutiles, parfois nuisibles?

N'est-on pas allé jusqu'à préconiser l'emploi d'autant d'alphabets indépendants qu'il y a de lettres à chiffrer? N'a-t-on pas publié des méthodes présentant, sous une forme ou sous une autre, plusieurs milliers d'alphabets tant numériques que littéraux, qui se remplacent continuellement et transforment, tant le chiffrement que la lecture d'une dépêche, en un travail de galérien?

Ce n'est pas, ici, le lieu de discuter ces procédés, il suffit de les mentionner pour montrer que, si sûrs qu'ils soient, ils n'ont rien de commun avec la cryptographie *pratique* qui seule peut véritablement prendre le nom de cryptographie.

De même que tout peut servir à transmettre la pensée, tout peut servir à la dissimuler : une liste d'objets quelconques se transforme aisément en nomenclature militaire ou politique; l'apparition et l'extinction de feux ou fanaux, le lancement de

fusées, le tir du fusil ou du canon, le son des cloches, etc., peuvent servir à correspondre ouvertement ou secrètement, soit directement par les signaux mêmes, soit accessoirement par la durée des intervalles séparant ces signaux; les encres sympathiques dissimulent même l'existence de l'écriture..., mais, là encore, ce n'est pas de la vraie cryptographie.

Par *cryptographie*, on doit entendre la *science* de transformer un texte clair en texte secret à l'aide de conventions préétablies, qui permettront ultérieurement au destinataire de reconstituer le texte clair à l'aide du texte secret.

Je dis que la cryptographie est une *science et non un art*; en effet, si habile qu'il soit, un chiffreur à qui on donne un texte à chiffrer, à l'aide d'une méthode et d'une clé déterminées, ne peut trouver qu'*une seule et unique* version du texte imposé. Il lui suffit donc de faire un travail analogue aux opérations arithmétiques et il ne peut y rien changer, sans rendre le cryptogramme inintelligible à ses correspondants.

Jusqu'à présent, il n'existe qu'une seule exception : la méthode dite à clé brisée ou à arrêts variables permet à l'expéditeur de faire varier la contexture des cryptogrammes sans en compromettre la traduction. Ce résultat est obtenu par l'application d'un principe ou d'une loi qu'il y aurait toute utilité à généraliser.

Il est donc incontestable que, bien que le *déchiffrement* tienne à la fois de la science et de l'art, le *chiffrement* ressortit exclusivement à la science.

La méconnaissance de ce fait est la seule cause du peu de progrès faits par la cryptographie. La plupart des traités ne sont, en quelque sorte, que des catalogues plus ou moins complets et détaillés de systèmes divers, dont aucun n'est étudié à fond, aussi plusieurs d'entre eux ne diffèrent qu'en apparence.

J'ai donc cru faire une œuvre utile en groupant tous ces systèmes et en les discutant de manière à en déduire les principes.

Ces principes établis, je me suis efforcé d'obvier à leurs inconvénients et de corriger leurs défauts, dès longtemps reconnus et particulièrement signalés par MM. Kerckhoffs, de Viaris, Valério, etc.

J'ai dû, dans le cours de ce travail, abandonner certaines expressions qui m'ont semblé impropres, telles que : clé simple, double, etc. En revanche, j'ai été conduit à créer de nouveaux mots pour exposer des idées ou nouvelles, ou considérées à un nouveau point de vue.

Afin de ne pas dérouter les cryptologues, j'ai exposé, plus ou moins sommairement, les principales méthodes connues, en rappelant le nom des inventeurs, mais en rattachant chaque procédé au principe dont il découle et en m'abstenant de toute critique, tout en indiquant, parfois, les perfectionnements dont ces systèmes semblent susceptibles.

En résumé, j'ai la conscience d'avoir fait un travail sérieux qui, je l'espère du moins, pourra rendre de bons services, malgré ses imperfections et ses lacunes.

Beaucoup de celles-ci sont dues à la nécessité de me restreindre, car, pour entrer dans tous les détails pratiques, chaque partie de ce travail exigerait un développement qui lui donnerait une importance égale à celle du présent volume.

Une dernière observation : la cryptographie *littérale*, la seule dont il soit question ici, semble peu utile à beaucoup de personnes familiarisées avec l'emploi des vocabulaires et dictionnaires chiffrés ; c'est cependant à cette cryptographie qu'elles devront avoir recours lorsque, tout en visant à l'économie télégraphique, elles voudront, en même temps, soustraire leurs correspondances à la connaissance d'intermédiaires indiscrets ou mal intentionnés. Le texte à cryptographier, au lieu d'être une phrase en langage ordinaire, sera alors une série de nombres ou de lettres fournie par un répertoire, mais les principes de chiffrage ne seront pas changés. Ils peuvent cependant, dans ce cas, être simplifiés et facilités, ainsi que je le démontrerai peut-être un jour.

Paramé, 25 mai 1901.

F. DELASTELLE.

TRAITÉ ÉLÉMENTAIRE

DE

CRYPTOGRAPHIE

DÉFINITIONS

On appelle *cryptographie* la *science* qui a pour objet l'étude des moyens susceptibles d'assurer le secret des correspondances ou écrits qu'on a intérêt à soustraire à la curiosité des tiers ou à l'indiscrétion des intermédiaires.

En d'autres termes, la *cryptographie* enseigne à transformer un *langage clair* en *langage secret*.

Le *langage clair* est celui dans lequel tous les mots de la langue employée ont leur signification réelle conforme au génie de la langue.

Le *langage secret* comprend le langage *convenu* et le langage *chiffré*.

On entend par *langage convenu* l'emploi des mots qui, tout en présentant chacun isolément un sens intrinsèque, ne forment point de phrases compréhensibles et ont, par suite d'une *convention*, une signification autre que celle qu'ils possèdent dans le langage ordinaire.

Le *langage chiffré* est celui dans lequel on emploie des *chiffres* au lieu des signes orthographiques usités dans le langage clair.

En cryptographie, on désigne par *chiffre* le caractère : chiffre, lettre ou signe conventionnel quelconque, employé pour représenter une lettre, un mot ou une phrase de langage clair.

De là le nom d'*écriture chiffrée* que l'on donne parfois à la cryptographie.

On appelle *conventions* les dispositions arrêtées entre deux ou plusieurs personnes relativement aux moyens à employer pour *chiffrer* un texte clair, c'est-à-dire le transformer en texte secret et pour *traduire* le texte chiffré en texte clair.

C'est à tort que l'on donne généralement à cette dernière opération le nom de *déchiffrement*. Par *déchiffrement*, il convient d'entendre la *traduction* d'un *cryptogramme* dont on ne connait pas la clé.

Un *cryptogramme* est un écrit en caractères secrets ou encore en caractères usuels disposés dans un ordre anormal.

La *clé* d'un cryptogramme est l'ensemble des conventions qui ont servi à opérer le chiffrement : système choisi, mode d'emploi, etc.

Un *cryptographe* est celui qui exécute les diverses opérations de la cryptographie. On l'appelle encore *chiffreur* et *traducteur*. On a proposé le nom de *cryptophote* pour le *déchiffreur ignorant la clé*, que M. de Viaris désigne aussi sous le nom de l'*ennemi*.

ou décrypteur, décryptement

On a étendu la dénomination de *cryptographe* à certains appareils permettant d'effectuer mécaniquement une partie des opérations de la cryptographie.

Toutes les écritures humaines sont ou idéographiques comme celle des Chinois, ou syllabiques comme celle des Japonais, ou alphabétiques comme celle des Européens.

En cryptographie, nous retrouvons les mêmes types d'écriture : les répertoires et les dictionnaires spéciaux servent à convertir les syllabes, les mots ou même les phrases en nombres, combinaisons de lettres ou mots conventionnels, qu'il sera souvent nécessaire de cryptographier eux-mêmes. Il en résulte qu'un traité élémentaire de cryptographie doit commencer par faire connaitre les divers moyens à employer pour cryptographier les chiffres ou lettres indépendamment de la signification secrète qu'ils peuvent posséder.

Nous nous occuperons donc exclusivement de la cryptographie littérale ou alphabétique.

Jusqu'à ces derniers temps, les procédés cryptographiques pouvaient se classer en :

1° Systèmes de transposition ;

2° Systèmes de substitution.

En 1893 (1), un nouveau procédé complètement différent a été mis en lumière, c'est la *méthode des polygrammes* qui, à une grande facilité d'écriture et de lecture, joint une sécurité jusqu'à présent absolue.

(1) *Cryptographie nouvelle*, par F. Delastelle. Paris, Dubreuil, 1893.

PREMIÈRE PARTIE

INVERSION OU TRANSPOSITION

L'*inversion* consiste à *transposer* ou déplacer les lettres du texte clair suivant une méthode convenue entre les correspondants, de telle sorte qu'il soit facile aux initiés de rétablir l'ordre primitif.

De nombreux systèmes ont été imaginés dans ce but :

1° Renversement des lettres;
2° Groupements divers;
3° Carrés et grilles;
4° Méthodes diverses.

Renversement. — Le *renversement* s'effectue en écrivant les lettres du clair en sens inverse de l'ordre normal, la dernière lettre devenant la première, l'avant-dernière la seconde, l'antepénultième la troisième, etc.

Exemple : *Paul est parti pour Lyon*, s'écrira :

NOYLRUOPITRAPTSELUAP

Le renversement peut s'appliquer soit au texte entier, soit successivement à chaque mot ou à des groupes d'un nombre de lettres convenu. La phrase ci-dessus, divisée en deux groupes de dix lettres, donnerait :

RAPTSELUAPNOYLRUOPIT

Et en quatre groupes de cinq lettres :

ELUAPRAPTSUOPITNOYLR

Il est évident que le renversement ne donne aucune sécurité au point de vue du secret, les dépêches écrites dans ce système ne résistant pas à un examen un peu sérieux.

Groupement. — Le *groupement* consiste à établir avec le texte clair un tableau d'une forme déterminée, où les lettres sont disposées suivant des lignes horizontales et des colonnes verticales bien définies. Ces lettres relevées ensuite dans un ordre convenu constituent le cryptogramme.

Méthode des diviseurs. — Dans cette méthode, les rangées horizontales possèdent toutes un même nombre de lettres ; il en est de même des colonnes verticales, la dernière rangée du texte étant, au besoin, complétée par l'addition de lettres *nulles* ou réduite par des abréviations opérées dans le texte, avec assez de soin pour ne pas altérer le sens.

Le tableau ainsi obtenu a la forme d'un rectangle, dont habituellement le nombre des colonnes est seul fixé par les conventions. Ces conventions pourraient tout aussi bien porter sur le nombre des rangées, la longueur de celles-ci variant selon l'étendue des dépêches.

Le tableau est *simple* ou *naturel*, lorsque les lignes horizontales sont toutes écrites de *gauche à droite*; il est *alterné*, lorsque la première rangée étant écrite de *gauche à droite*, la seconde l'est de *droite à gauche*, etc., de telle sorte que les rangées de rang impair vont dans une direction et celle de rang pair dans la direction inverse, si bien que le texte semble former une ligne continue, repliée sur elle-même, mode d'écrire que les Grecs désignaient par le nom de *boustrophèdon*.

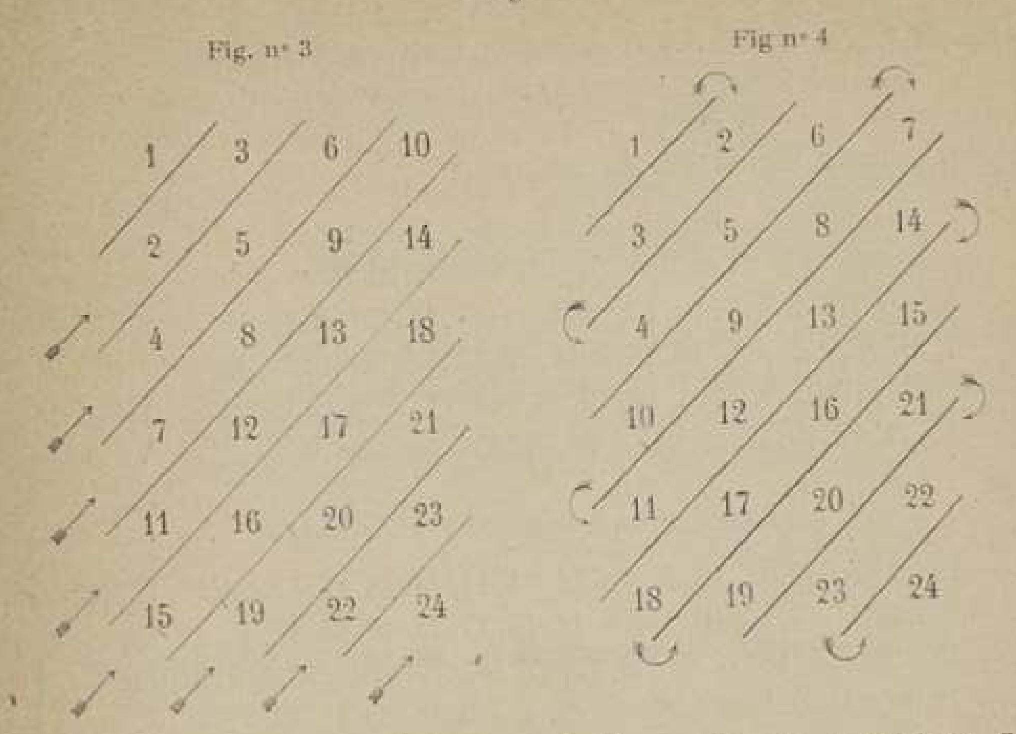
Le tableau est *diagonal*, quand on écrit en partant d'un angle et en remplissant les cases des diverses lignes parallèlement à la diagonale du carré formé par les n premières rangées et les n premières colonnes. Suivant que l'on emploie pour l'inscription des lettres dans ce système, l'ordre simple ou alterné, le tableau diagonal est dit *simple* ou *alterné*.

Fig. n° 1

→	1	2	3	4
→	5	6	7	8
→	9	10	11	12
→	13	14	15	16
→	17	18	19	20
→	21	22	23	24

Fig. n° 2

→	1	2	3	4
	8	7	6	5
	9	10	11	12
	16	15	14	13
	17	18	19	20
	24	23	22	21



Le *relèvement* peut s'effectuer de beaucoup de manières. On distingue les relèvements en *réguliers* et *irréguliers*.

Les *relèvements réguliers* se divisent en : *naturel* et *diagonal* ; chacun d'eux, à son tour, se subdivise en *simple* et *alterné*.

Le relèvement *naturel* consiste à inscrire horizontalement les lettres composant les colonnes verticales. Il est *simple* si chaque colonne est relevée à la suite de la précédente et dans le même sens ; il est *alterné* si chaque colonne, relevée à la suite de la précédente, est prise dans le sens inverse.

Les lettres, qui, dans les tableaux ci-dessus, sont représentées par leurs numéros d'ordre, donneraient les résultats suivants :

RELÈVEMENT NATUREL SIMPLE.

N° 1. — 1, 5, 9, 13, 17, 21, 2, 6, 10, 14, 18, 22, 3, 7, 11, 15, 19, 23, 4, 8, 12, 16, 20, 24.
N° 2. — 1, 8, 9, 16, 17, 24, 2, 7, 10, 15, 18, 23, 3, 6, 11, 14, 19, 22, 4, 5, 12, 13, 20, 21.
N° 3. — 1, 2, 4, 7, 11, 15, 3, 5, 8, 12, 16, 19, 6, 9, 13, 17, 20, 22, 10, 14, 18, 21, 23, 24.
N° 4. — 1, 3, 4, 10, 11, 18, 2, 5, 9, 12, 17, 19, 6, 8, 13, 16, 20, 23, 7, 14, 15, 21, 22, 24.

RELÈVEMENT NATUREL ALTERNÉ.

N° 1. — 1, 5, 9, 13, 17, 21, 22, 18, 14, 10, 6, 2, 3, 7, 11, 15, 19, 23, 24, 20, 16, 12, 8, 4.
N° 2. — 1, 8, 9, 16, 17, 24, 23, 18, 15, 10, 7, 2, 3, 6, 11, 14, 19, 22, 21, 20, 13, 12, 5, 4.
N° 3. — 1, 2, 4, 7, 11, 15, 19, 16, 12, 8, 5, 3, 6, 9, 13, 17, 20, 22, 24, 23, 21, 18, 14, 10.
N° 4. — 1, 3, 4, 10, 11, 18, 19, 17, 12, 9, 5, 2, 6, 8, 13, 16, 20, 23, 24, 22, 21, 15, 14, 7.

Le relèvement *diagonal* s'opère obliquement. Comme le précédent, il peut être *simple* ou *alterné*.

Appliqué aux tableaux ci-dessus, il donnerait aux lettres les

dispositions ci-après. — Il convient de remarquer que le relèvement diagonal, simple ou alterné, des tableaux diagonaux doit commencer par un angle autre que celui qui a servi de point de départ pour la formation du tableau.

RELÈVEMENT DIAGONAL SIMPLE.

N° 1. — 1, 2, 5, 3, 6, 9, 4, 7, 10, 13, 8, 11, 14, 17, 12, 15, 18, 21, 16, 19, 22, 20, 23, 24.
N° 2. — 1, 2, 8, 3, 7, 9, 4, 6, 10, 16, 5, 11, 15, 17, 12, 14, 18, 24, 13, 19, 23, 20, 22, 21.
N° 3. — 15, 11, 19, 7, 16, 22, 4, 12, 20, 24, 2, 8, 17, 23, 1, 5, 13, 21, 3, 9, 18, 6, 14, 10.
N° 4. — 18, 11, 19, 10, 17, 23, 4, 12, 20, 24, 3, 9, 16, 22, 1, 5, 13, 21, 2, 8, 15, 6, 14, 7.

RELÈVEMENT DIAGONAL ALTERNÉ.

N° 1. — 1, 5, 2, 3, 6, 9, 13, 10, 7, 4, 8, 11, 14, 17, 21, 18, 15, 12, 16, 19, 22, 23, 20, 24.
N° 2. — 1, 8, 2, 3, 7, 9, 16, 10, 6, 4, 5, 11, 15, 17, 24, 18, 14, 12, 13, 19, 23, 22, 20, 21.
N° 3. — 15, 19, 11, 7, 16, 22, 24, 20, 12, 4, 2, 8, 17, 23, 21, 13, 5, 1, 3, 9, 18, 14, 6, 10.
N° 4. — 18, 19, 11, 10, 17, 23, 24, 20, 12, 4, 3, 9, 16, 22, 21, 13, 5, 1, 2, 8, 15, 14, 6, 7.

Diverses modifications peuvent être apportées aux opérations exposées ci-dessus ; ainsi la formation des tableaux et leur relèvement ou l'un ou l'autre, peuvent avoir un point de départ autre que celui indiqué ; ils peuvent également se faire d'une manière toute différente, par exemple, en hélice, en prélevant les lettres qui forment la bordure des parallélogrammes et en infléchissant vers le centre, ou inversement en partant du centre, etc.

La méthode des diviseurs est dite *irrégulière* lorsque, avant de procéder au relèvement, on transpose les colonnes ou les rangées, ou même les deux, au lieu de les laisser dans leur ordre naturel; le relèvement se fait ensuite suivant l'un des procédés exposés ci-dessus.

Afin de soulager la mémoire, qui retient difficilement une suite de chiffres, on choisit habituellement, comme clé, un ou deux mots, suivant le cas. Le rang alphabétique de chaque lettre indique l'ordre à donner aux rangées et aux colonnes. Soit le mot PARIS; les lettres se numéroteront d'après l'ordre alphabétique relatif : A=1, I=2, P=3, R=4, S=5, et fourniront la suite 3.1.4.2.5. en inscrivant sous chaque lettre du mot le chiffre qui lui correspond :

P A R I S
3 1 4 2 5

De même, le mot FRANCE donnera 4.6.1.5.2.3 :

F R A N C E
4 6 1 5 2 3

Supposons que l'on veuille chiffrer la phrase :

Partez immédiatement pour Avignon.

Les conventions supposées portent qu'on écrira sur six colonnes ; que ces colonnes seront transposées d'après les chiffres indiqués par le mot FRANCE et que le mot PARIS servira à transposer les rangées.

PARIS n'ayant que cinq lettres, si le nombre des lignes est supérieur, on écrit le mot-clé plusieurs fois de suite, de façon à obtenir autant de lettres qu'il y a de rangées et on opère comme ci-dessus. Ainsi pour douze rangées on aurait :

P	A	R	I	S	P	A	R	I	S	P	A	
6	1	9	4	11	7	2	10	5	12	8	3	ou 6.1.9.4.11.7.2.10.5.12.8.3

Revenons à notre exemple et formons le tableau suivant :

N° 1

	1	2	3	4	5	6
1	p	a	r	t	e	z
2	i	m	m	e	d	i
3	a	t	e	m	e	n
4	t	p	o	u	r	a
5	v	i	g	n	o	n

Utilisant ensuite les clés, nous intervertissons successivement l'ordre des colonnes, puis celui des rangées, ou *vice versa*, et obtenons finalement le tableau n° 3 :

N° 2

	4	6	1	5	2	3
1	t	z	p	e	a	r
2	e	i	i	d	m	m
3	m	n	a	e	t	e
4	u	a	t	r	p	o
5	n	n	v	o	i	g

N° 3

	4	6	1	5	2	3
3	m	n	a	e	t	e
1	t	z	p	e	a	r
4	u	a	t	r	p	o
2	e	i	i	d	m	m
5	n	n	v	o	i	g

dont le relèvement s'effectuera d'après une méthode quelconque, mais fixée par les conventions.

Avec le relèvement naturel vertical simple, la dépêche serait :

mtuennzainaptiveerdotapmieromg.

On aurait pu opérer inversement et donner au premier tableau

les numéros fournis par les mots-clés, puis dépouiller suivant l'ordre naturel des nombres. On aurait alors obtenu :

N° 1

	4	6	1	5	2	3
3	p	a	r	t	e	z
1	i	m	m	e	d	i
4	a	t	e	m	e	n
2	t	p	o	u	r	a
5	v	i	g	n	o	n

N° 2

	1	2	3	4	5	6
3	r	e	z	p	t	a
1	m	d	i	i	e	m
4	e	e	n	a	m	t
2	o	r	a	t	u	p
5	g	o	n	v	n	i

N° 3

	1	2	3	4	5	6
1	m	d	i	i	e	m
2	o	r	a	t	u	p
3	r	e	z	p	t	a
4	e	e	n	a	m	t
5	g	o	n	v	n	i

et la dépêche, relevée comme ci-dessus, serait :

moregdreeoiaznnitpaveutmnmpati,

résultat identique avec celui qu'auraient donné, par la première méthode, les clés numériques : 3, 5, 6, 1, 4, 2, et 2, 4, 1, 3, 5.

Toutes ces méthodes, d'une conception simple mais d'une application longue et délicate, sinon pénible, offrent peu de garanties d'indéchiffrabilité. Un déchiffreur sagace et exercé éprouvera généralement peu de difficultés à pénétrer le sens des dépêches écrites dans ce système. Sa tâche sera grandement facilitée par les diverses particularités de la langue employée, ainsi que par les imperfections des méthodes ci-dessus exposées.

Ces imperfections ou défectuosités ont été jugées assez graves pour que le *Dictionnaire militaire*, qui préconise le dernier système que nous avons étudié, insiste fortement sur l'adjonction au texte à cryptographier de nombreuses lettres *nulles*, ayant pour objet de dérouter les recherches de l'ennemi. Nous verrons plus loin, en traitant du déchiffrement que cette garantie est illusoire.

Au lieu d'introduire des *nulles*, qui ont l'inconvénient d'allonger le travail du chiffrement et celui de la traduction et, parfois, de laisser subsister un doute sur l'étendue de la dépêche, sans, pour cela, augmenter sensiblement les difficultés du déchiffrement, il vaut mieux laisser sans emploi un certain nombre de cases déterminées par convention et, à défaut de convention spéciale, les dernières du tableau.

Ce mode de procéder n'augmente pas le travail du chiffreur, ni celui du traducteur et présente le grand avantage de ne fournir à l'ennemi aucune indication sur le nombre des colonnes ou des rangées, ce qui accroît notablement les difficultés du tâtonnement.

Chaque lettre manquante étant remplacée par un point, aucun changement n'est apporté au chiffrement habituel ; mais les points auxiliaires ne faisant pas partie de la dépêche transmise,

l'ordre des lettres est troublé et le déchiffrement se trouve, de ce chef, rendu plus difficile.

Soit à traduire la dépêche suivante chiffrée dans ces conditions :

lvlttnianurtfearihoesnseauoeus.

Notons, en passant, que 31, total des lettres de cette dépêche, est un nombre premier et n'a point de diviseurs.

Pour nous, sachant que le nombre des colonnes est sept, nous en déduirons que celui des rangées est cinq et que l'une d'elles ne renferme que trois lettres ; il y a donc *quatre vides*. Aucune convention n'ayant été faite à ce sujet, ces vides doivent se trouver à la fin de la dépêche, c'est-à-dire sur la cinquième rangée, dans les colonnes 4, 5, 6, et 7.

Préparons maintenant le damier destiné à former le tableau servant de début à la traduction. Écrivons sur son pourtour les chiffres choisis pour clés ; puis biffons d'un trait de plume les cases qui doivent rester vides ; nous aurons :

	6	1	3	5	7	4	2
4							
1							
5	×			×	×	×	
3							
2							

Il ne reste plus qu'à inscrire les lettres de la dépêche, colonne par colonne et du haut en bas, dans les cases disponibles, pour obtenir le tableau suivant :

	6	1	3	5	7	4	2
4	l	t	n	e	h	n	u
1	v	n	u	a	o	s	o
5	×	i	r	×	×	×	e
3	l	a	t	r	e	e	u
2	t	n	f	i	s	a	s

qui, après transposition des colonnes et des rangées, deviendra :

	1	2	3	4	5	6	7
1	n	o	u	s	a	v	o
2	n	s	f	a	i	t	s
3	a	u	t	e	r	l	e
4	t	u	n	n	e	l	h
5	i	e	r	×	×	×	×

et on lit clairement : *Nous avons fait sauter le tunnel hier.*

Soit encore à traduire :

ptsrereonpslsoesnta,

sachant que la première case des trois premières rangées est vide ; que 5 est le nombre des colonnes et que la même clé numérique : 5.1.3 2 4 a été employée dans les deux sens.

Si, à 19, nombre des lettres de la dépêche, nous ajoutons 3 pour les cases vides du commencement, nous trouvons le total 22, que nous divisons par 5, nombre des colonnes. Le quotient est 4 et on a 2 pour reste ; nous en concluons que le tableau primitif contient cinq rangées dont l'une renferme trois vides. Ces trois vides n'étant pas expressément prévus par les conventions ne peuvent se trouver qu'à la fin de la dépêche claire, soit sur la cinquième rangée, colonnes : 3, 4 et 5. — Les vides prévus sont dans la première colonne, rangées : 1, 2 et 3.

Nous pouvons donc biffer sur le damier préparé les cases vides, puis remplir les autres suivant les conventions arrêtées, et nous aurons :

	5	1	3	2	4
5	X	e	·	s	X
1	p	X	e	l	s
3	t	X	o	s	n
2	s	X	n	o	t
4	r	r	p	e	a

et, après double transposition :

	1	2	3	4	5
1	X	l	e	s	p
2	X	o	n	t	s
3	X	s	o	n	t
4	r	e	p	a	r
5	e	s	X	X	X

ce qui donne le texte clair : *Les ponts sont réparés.*

Le principal défaut que l'on reproche à la *méthode des diviseurs* c'est que les groupes, soit verticaux, soit horizontaux, ne se mélangent jamais, ce qui limite notablement les recherches et tâtonnements en vue du déchiffrement sans clé.

L'emploi des cases vides remédie à ce défaut capital. Il présente le double avantage :

1° De ne fournir aucune indication sur les nombres qui servent à la formation du tableau ;

2° De masquer l'importance ou l'étendue de chaque groupe, en leur attribuant des nombres de lettres différents, ce qui conduit forcément le déchiffreur à faire chevaucher ces groupes l'un sur l'autre, tandis que le traducteur, connaissant la clé, n'éprouvera, comme nous venons de le voir, aucune difficulté à les classer normalement.

Carrés. — Les carrés, dont la forme du reste peut, sans nul inconvénient, être modifiée et se transformer en losange, rectangle ou toute autre figure géométrique, sont divisés en cases

régulièrement disposées et portant des numéros qui servent à indiquer la place que doit occuper chaque lettre.

Afin d'éviter le groupement des lettres voisines, qui se produit forcément dans la méthode précédente, chacun des numéros à inscrire dans les cases d'un carré est arbitrairement choisi, tiré au sort, ou déterminé par une convention ou méthode quelconque, mais de telle sorte que les nombres se suivent dans un ordre ne présentant aucune liaison, aucune symétrie et dû, en apparence du moins, au simple hasard.

Soit, par exemple, le carré :

4	13	6	11
1	16	7	10
15	2	9	8
14	3	12	5

Nous en extrairons les deux suites :

A.. .. 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16
B... . 4, 13, 6, 11, 1, 16, 7, 10, 15, 2, 9, 8, 14, 3, 12, 5

La première, A, suite naturelle des nombres, n'est que le numérotage des cases du tableau ; la seconde, B, présente les nombres attribués à chacune de ces cases par un procédé quelconque.

Pour chiffrer, nous écrirons chaque terme de l'une des suites sous chacune des lettres à cryptographier ; puis nous transposerons selon les indications de la deuxième suite. Exemple :

I l a r r i v e r a d e m a i n
A..... 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16

s'écrira :

B..... 4 13 6 11 1 16 7 10 15 2 9 8 14 3 12 5
r m i d i n v a i l r e a a e r

En attribuant la suite B au clair, on aurait trouvé pour cryptogramme :

A..... 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16.
r a a i n a v e d e r i l m r i

La traduction étant toujours l'opération inverse du chiffrement, on emploiera la deuxième méthode pour la lecture des dépêches cryptographiées à l'aide de la première et, réciproque-

ment, on se servira de la première méthode pour traduire les cryptogrammes écrits avec la seconde.

La forme de parallélogrammes rectangulaires, sous laquelle on écrit habituellement les suites de ce genre, a pour but de faciliter les modifications à apporter à la série primitive, afin de mieux assurer le secret de la correspondance.

Ces modifications se font généralement par la transposition des colonnes et des rangées, de la manière exposée, pour les lettres, à la méthode des diviseurs irrégulière. On ne saurait trop recommander d'ajouter aux déplacements habituels le retournement, bout pour bout, de quelques bandes, tant horizontales que verticales.

L'emploi de ces séries ou suites de nombres est lent, pénible, et exige d'autant plus d'attention qu'elles sont plus longues ; or, quand on est conduit à employer des séries de plusieurs centaines de nombres, on reconnait promptement que la méthode des carrés n'est pas d'un emploi pratique.

Grilles. — Les *grilles*, inventées, dit-on, par Jérôme Cardan et très usitées au XVIIIe siècle, étaient abandonnées, leur emploi étant incompatible avec le télégraphe, puisqu'elles ne pouvaient servir qu'en s'appliquant sur le texte original.

L'emploi de ces appareils pour la correspondance télégraphique est devenu facile depuis les travaux de MM. Kluber, Martens, Fleissner von Wostrowitz et de Viaris.

On est parti de ce fait que, si on a deux carrés identiques divisés en un nombre quelconque de cases égales et que, l'un de ces carrés restant fixe, on fasse successivement coïncider avec ses quatre côtés, un même côté du carré mobile, chaque case du second carré en recouvre successivement quatre du premier. Il suffit donc de déterminer la position de $\frac{n}{4}$ cases convenablement choisies pour avoir un carré complet de n cases. En effet, considérons les deux carrés ci-dessous :

N° 1

19	20	21	22	23	24
18	6	7	8	9	25
17	5	1	2	10	26
36	16	4	3	11	27
35	15	14	13	12	28
34	33	32	31	30	29

N° 2

g	h	i			
f	c	d			
e	b	a			

Il est manifeste que, pendant la rotation du second sur le premier, chacune des cases *a*, *b*, *c*, etc., recouvrira successivement celles du premier indiquées au tableau ci-après :

N° 3

Carré central	1re bande			2e bande				
a	b	c	d	e	f	g	h	i
1	5	6	7	17	18	19	20	21
2	8	9	10	22	23	24	25	26
3	11	12	13	27	28	29	30	31
4	14	15	16	32	33	34	35	36

Il n'est peut-être pas inutile de faire remarquer que, dans les carrés numérotés comme le précédent, les numéros des cases appartenant à une lettre quelconque forment une progression arithmétique dont la raison est : 1 pour le carré central, 3 pour la première bande rectangulaire qui l'enveloppe immédiatement, 5 pour la deuxième bande, 7 pour la troisième et, en général $2n + 1$ pour la n^e bande.

Dans les carrés d'un nombre *impair* de cases, le centre est formé d'une seule case et les numéros des cases des bandes quadrangulaires, comptées à partir du centre, forment une progression arithmétique dont la raison est représentée par $2n$, n indiquant le rang de la bande considérée.

Ceci posé, prenons une feuille de carton, de tôle mince, etc. ; traçons dessus un damier et inscrivons-y des numéros d'ordre disposés comme dans la figure numéro 1.

Choisissons maintenant, dans le tableau numéro 3, un des nombres ressortissant à chaque lettre, de manière que les cases qu'ils représentent soient aussi disséminées que possible et surtout que deux de ces cases *ne soient jamais juxtaposées ni verticalement, ni horizontalement*. Découpons à jour les cases choisies et l'appareil sera terminé.

En résumé, une *grille* consiste en une feuille percée de trous ou fenêtres disposés de telle sorte qu'en appliquant cette feuille, dans *quatre* positions différentes, sur un damier de mêmes dimensions, toutes les cases de ce damier soient successivement découvertes par les fenêtres de la grille.

Au fond, les grilles produisent un numérotage mécanique des cases d'un carré, avec cette différence toutefois que si les numéros d'un carré peuvent être absolument indépendants les uns des autres, il n'en est plus ainsi de ceux obtenus à l'aide d'une grille, ce qui est un défaut. Mais l'emploi des grilles facilite

beaucoup le chiffrement et nous verrons bientôt qu'il n'est pas impossible de supprimer presque complètement la solidarité entre les différents numéros.

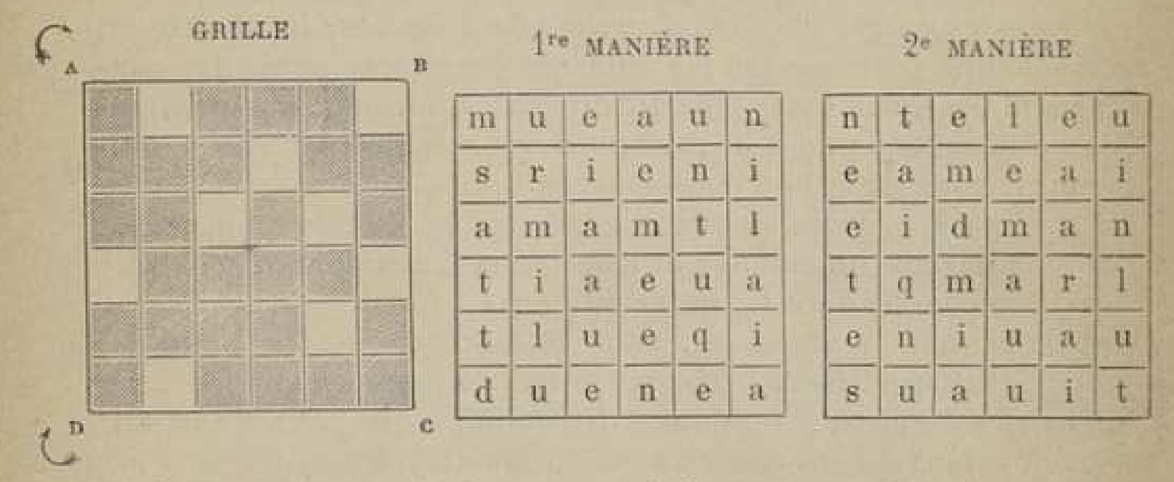
Comme pour les carrés, le chiffrement à l'aide d'une grille peut se faire de deux manières :

Première manière. — Poser la grille sur un damier de mêmes dimensions que l'appareil ; inscrire dans chaque ouverture une lettre du texte clair, en suivant l'ordre du texte ; toutes les fenêtres étant remplies, faire tourner la grille de 90° dans le sens convenu et remplir les nouvelles cases découvertes en y inscrivant les lettres claires qui suivent, etc., puis relever selon les conventions les lettres du carré ainsi formé.

Deuxième manière. — Écrire chaque lettre claire dans les cases du damier en suivant l'ordre du texte et en se conformant aux conventions pour remplir le damier, soit de haut en bas, etc., soit plus simplement de gauche à droite. Placer ensuite la grille dans sa position de début et relever successivement dans l'ordre normal les lettres qui apparaissent aux ouvertures.

Exemple : soit à chiffrer :

Une attaque simulée aura lieu demain matin.



1re MANIÈRE

m	u	e	a	u	n
s	r	i	e	n	i
a	m	a	m	t	l
t	i	a	e	u	a
t	l	u	e	q	i
d	u	e	n	e	a

2e MANIÈRE

n	t	e	l	e	u
e	a	m	e	a	i
e	i	d	m	a	n
t	q	m	a	r	l
e	n	i	u	a	u
s	u	a	u	i	t

La *deuxième* méthode sert pour la lecture quand le chiffrement a été fait avec la *première*, et, réciproquement, la *première* méthode doit être employée pour la traduction des dépêches écrites avec la *seconde*, en remplaçant, dans la règle ci-dessus, les mots : *texte clair* par *texte chiffré*.

La rotation de la grille se fait indifféremment de droite à gauche ou de gauche à droite, suivant les conventions. Dans les deux systèmes, la première et la troisième positions donnent un résultat identique ; la deuxième et la quatrième ne modifient que la place à laquelle se présente, à la lecture, la ligne des lettres chiffrées dans chacune de ces positions.

Au lieu de faire tourner la grille, on peut la *renverser*, mais

la disposition des ouvertures qui convient pour la rotation peut ne pas permettre le retournement. Le tableau ci-après donne la situation des ouvertures dans ce dernier système.

Centre	1re bande			2e bande					3e bande					
a	b	c	d	e	f	g	h	i	j	k	l	m	n	.
1	5	6	7	17	18	19	20	21	37	38	39	40	41	...
2	10	9	8	26	25	24	23	22	50	49	48	47		
3	11	12	13	27	28	29	30	31	51	52	53			
4	16	15	14	36	35	34	33	32	64	63				

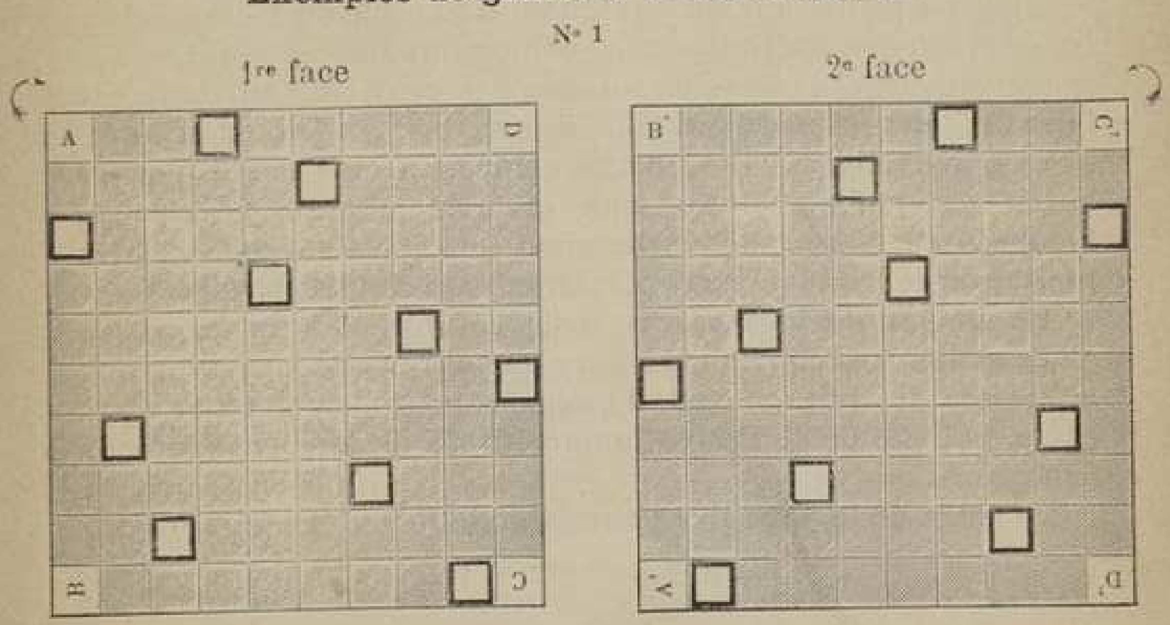
La loi de formation de ces suites est facile à reconnaitre.

En rapprochant ce tableau de celui numéro 3 (page 17), on constate que les colonnes du milieu et les première et troisième rangées de toutes les bandes sont identiques ; il en résulte que si les ouvertures d'une grille sont exclusivement choisies parmi ces suites, la grille pourra, à volonté, être utilisée par rotation ou par retournement ; mais il importe de faire remarquer que les cryptogrammes obtenus seront alors identiquement les mêmes dans les deux systèmes.

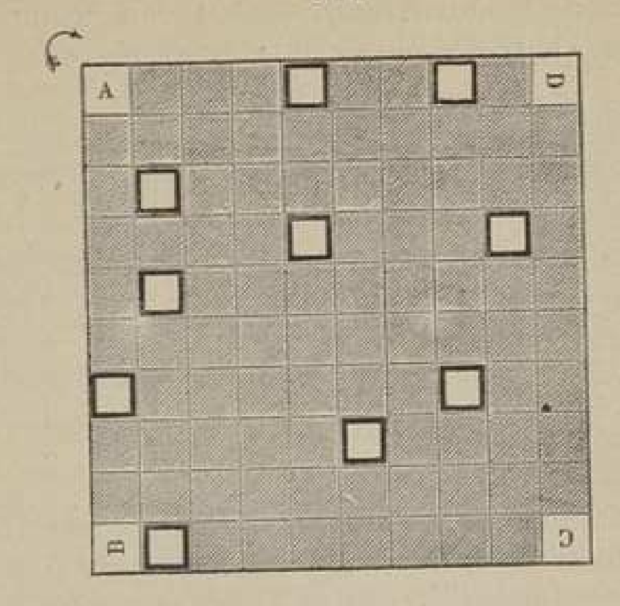
On peut cependant utiliser le renversement pour construire des grilles à *double rotation ;* chaque face de l'appareil fournissant, par rotation, quatre positions, le nombre total de celles-ci est de *huit*. Une seule ouverture permet donc de chiffrer huit lettres ; six ouvertures en chiffreront quarante-huit, dix suffiront pour quatre-vingts, quinze pour cent vingt, etc.

Exemples de grilles à double rotation.

N° 1



N° 2



CRYPTOGRAMMES A TRADUIRE :

Avec la grille numéro 1. — Au renversement, amener A' dans la position primitivement occupée par A : *ocerdderbztdrpnnlusn cutrrtoererveuoprlemiusrerznozeenefeipsuroueosroddottecehono.*

Avec la grille numéro 2. — Au renversement, rabattre A sur D, puis faire la deuxième rotation dans le même sens que la première : *unfuedtemdsianxlnmveatqseeraevpieaodilrohrneiun aeriedoenohusotrlidsseiurlltusner.* — Brizeux.

Pour traduire, la grille étant dans sa position initiale, inscrire dans chaque fenêtre une des dix premières lettres du cryptogramme, en suivant l'ordre normal ; faire tourner la grille d'un angle droit, inscrire les dix lettres suivantes, etc.

Avec les grilles à double rotation, il importe de bien préciser les conventions déterminant la position initiale, celle qui suit le renversement et le sens de rotation ; il convient, en outre, de faire toujours les deux rotations en sens inverse l'une de l'autre.

Ces nouvelles grilles, d'une confection plus facile que les anciennes et d'une plus grande sécurité, peuvent affecter de nombreuses formes et mériteraient une étude spéciale que les limites de ce traité ne nous permettent pas d'entreprendre.

Le tableau des ouvertures, indispensable pour la formation d'une grille, sert également à faire connaître cette formation aux intéressés. Il suffit, en effet, d'indiquer, pour chaque lettre de la grille, la ligne où se trouve le numéro de la case choisie pour fenêtre.

La grille de la page 18 a pour formule :

a, 1 — b, 2 — c, 3 — d, 2 — e, 3 — f, 4 — g, 2 — h, 1 — i, 4

ou, en supprimant les lettres, dont l'ordre est connu :

1, 2, 3, 2, 3, 4, 2, 1, 4,

ce que nous pouvons traduire en lettres, par exemple, par :

L. C. W. D. U. D ou A. W. W. D. B. N. etc.

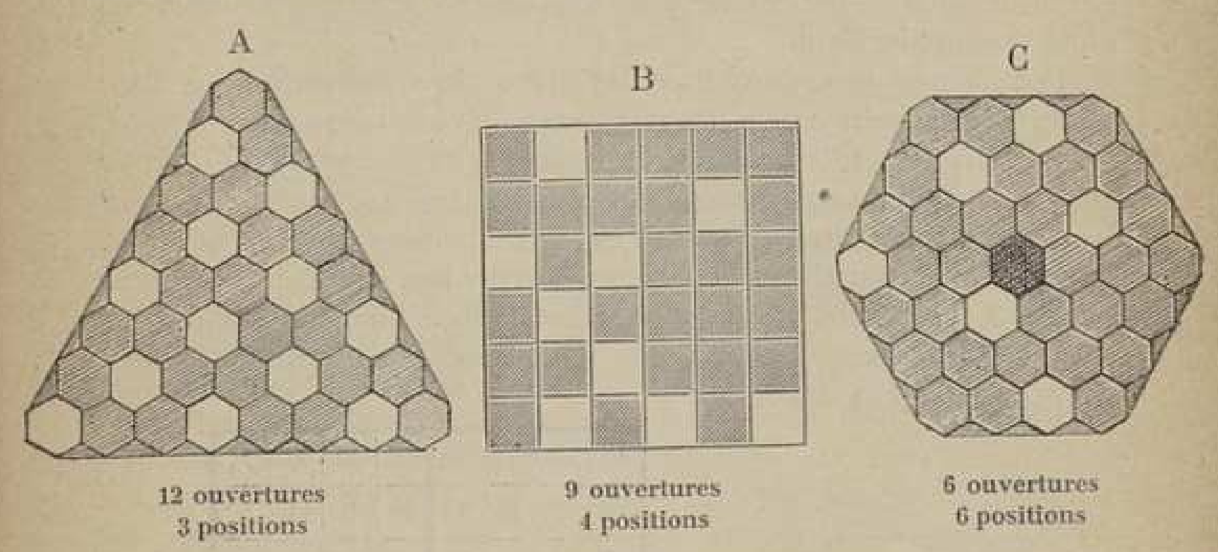
chaque lettre représentant les chiffres qui indiquent son rang dans l'alphabet : L = 12, C = 3, W = 23, D = 4, U = 21, etc.

Il importe de remarquer que toute grille d'un nombre pair de cases fournit, par son simple glissement sur un damier convenable, une nouvelle grille de dimension quelconque, supérieure ou inférieure à celle de la première. Les grilles impaires fournissent un résultat de même genre, mais l'étude approfondie de ces appareils sortirait du cadre que nous nous sommes tracé.

Les grilles peuvent affecter toutes les formes régulières : triangle, carré, pentagone, etc. Elles s'emploient alors par rotation et prennent autant de positions que le polygone a de côtés.

Les grilles en forme de rectangle (non carré), losange, etc., ne peuvent servir que par la méthode du retournement et l'emplacement de leurs ouvertures doit être calculé en conséquence.

Voici, à titre de simple curiosité, une même phrase cryptographiée avec trois grilles de formes différentes, employées par rotation de gauche à droite. — Première manière. Relevé horizontal par lignes successives :



12 ouvertures
3 positions

9 ouvertures
4 positions

6 ouvertures
6 positions

A : *llnteemsredeneprtbiaaitsrshepisaeorr;*
B : *alipreapreelsedmsreeiosnhtbinetartrs;*
C : *aalliestnetmissdhprereeeiaerpnstrobr.*

Il nous reste à rechercher le mode d'emploi des grilles capable d'assurer le mieux le secret des correspondances.

Il est évident que moins nous fournirons de renseignements au déchiffreur ennemi, plus ardue sera sa tâche ; il convient donc

d'éviter l'emploi d'une grille complète, ce qui est toujours facile dans un service de cryptographie bien organisé.

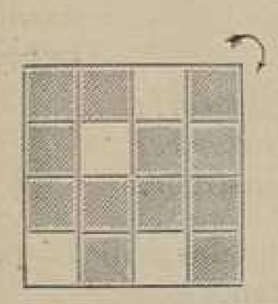
En effet, le nombre des lettres de la dépêche est *inférieur*, *égal* ou *supérieur* à celui des cases de la grille.

Dans le premier cas, aucune modification n'est apportée au chiffrement, qui prend fin dès que toutes les lettres claires ont été inscrites. Par contre, avant de commencer son travail, le traducteur doit biffer, sur le damier où il inscrira les lettres de la dépêche, un nombre de cases égal à la différence entre le total des cases du damier et celui des lettres du cryptogramme; les cases biffées étant, suivant les conventions, les premières ou mieux les dernières du damier, ou celles qui sont découvertes par les dernières ouvertures de la grille placée dans sa quatrième (ou toute autre) position, aucune difficulté ne peut se présenter, et la lecture se fait exactement comme si le tableau était complet.

Lorsque le nombre des lettres de la dépêche est *égal* ou *supérieur* à celui des cases de la grille, on prépare un tableau ou damier plus que suffisant pour contenir toutes les lettres à cryptographier et assez grand pour permettre à la grille de se déplacer parallèlement à elle-même, sans qu'une même case soit jamais recouverte deux fois dans ce mouvement.

Après avoir, s'il y a lieu, biffé les cases surabondantes, on procède au chiffrement en portant la grille, dans sa première position, successivement sur chacun des quartiers; puis, mettant la grille dans sa deuxième position, on en recouvre de nouveau chaque quartier, etc.

Proposons-nous, pour fixer les idées, de cryptographier, avec une grille de *seize* cases, une dépêche de cinquante-deux lettres. Le nombre des lettres étant supérieur à 48 ($=3\times16$), le damier sera formé de quatre quartiers de seize cases ($4\times16=64$). D'après les conventions supposées, les cases inutilisées devront affecter, d'abord, les dernières colonnes verticales, puis la dernière rangée horizontale. Le damier prendra donc l'aspect suivant, les lettres étant représentées par le numéro du rang qu'elles occupent dans la dépêche :



15	29	1	30	19	33	5	×
42	2	16	43	46	6	20	×
17	44	31	18	21	47	34	×
3	32	4	45	7	35	8	×
25	38	11	39	22	36	9	×
50	12	26	51	48	10	23	×
27	52	40	28	24	49	37	×
13	41	14	×	×	×	×	×

Avec la grille de trente-six cases ci-dessous et la convention qu'il ne sera tenu, *dans le chiffrement,* aucun compte des cases inutilisées comme superflues, ce qui obligera le traducteur à les rechercher par le maniement de la grille, on aurait obtenu le tableau :

×	37	1	19	×	38	×	46	10	28	×	47
2	20	×	39	3	21	11	29	×	48	12	30
40	×	22	4	41	×	49	×	31	13	50	×
23	5	42	×	24	6	32	14	51	×	33	15
×	43	7	25	×	44	×	52	16	34	×	×
8	26	×	45	9	27	17	35	×	×	18	36

Avec la même grille de trente-six et les conventions du premier exemple, on trouverait :

40	27	1	15	41	28	49	36	10	×	×	×
2	16	42	29	3	17	11	24	50	×	×	×
30	43	18	4	31	44	37	51	25	×	×	×
19	5	32	45	20	6	26	12	38	×	×	×
46	33	7	21	47	34	52	39	13	×	×	×
8	22	48	35	9	23	14	×	×	×	×	×

Ces exemples, qu'il serait facile de multiplier, semblent suffisants pour édifier le lecteur, qui remarquera que tout ce qui précède s'applique au premier mode d'emploi des grilles (page 18) et que, pour le deuxième mode, le travail du chiffreur devient celui du traducteur et réciproquement.

Un peu de pratique familiarisera promptement avec l'emploi rationnel des grilles, mais il est bon de noter que le moindre changement dans les conventions, dans la grille ou dans son maniement, peut modifier profondément la séquence des lettres du cryptogramme.

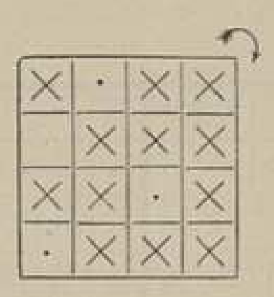
Les grilles fournissent, sans contredit, le meilleur moyen d'inversion des textes dont l'expédition en clair pourrait présenter des inconvénients. Mais la conservation de ces appareils peut offrir quelque danger et, bien que facile, leur perforation ne laisse pas d'être délicate et d'exiger un temps assez long, surtout

si l'on n'a pas à sa disposition d'emporte-pièce ou autre outil convenable. En attendant que nous puissions faire fabriquer les *grilles universelles* que nous avons imaginées, nous avons cherché le moyen d'éviter la perforation et nous pensons que les grilles *pleines* sont susceptibles de rendre d'utiles services.

Grilles non perforées. — Sur une feuille de papier quadrillé, nous pointons les cases que doivent occuper les fenêtres d'une grille conventionnelle, puis, sur une bande du même papier, nous reportons la première rangée de la grille, que nous faisons suivre de la deuxième, puis de la troisième et de la quatrième. Sous cette première ligne, nous en établissons une seconde formée de la même manière, après avoir mis la grille dans sa deuxième position ; une troisième ligne correspond à la troisième position, etc.

Note. — Pour les grilles carrées, la troisième ligne n'est que le renversement de la première, et la quatrième le renversement de la deuxième.

Exemple :



1re position.	×	·	×	×	·	×	×	×	×	×	·	×	·	×	×	×
2e —	·	×	·	×	×	×	×	·	×	·	×	×	×	×	×	×
3e —	×	×	×	·	×	·	×	×	×	×	×	·	×	×	·	×
4e —	×	×	×	×	×	×	·	×	·	×	×	×	×	·	×	·

Inscrivons les lettres de la dépêche à chiffrer, d'abord dans les cases vides de la première rangée, puis dans celles de la deuxième, de la troisième et enfin de la quatrième. Relevons ensuite les lettres suivant l'ordre des colonnes et nous obtiendrons le même cryptogramme que par l'emploi habituel de la grille.

. v . . o . . . . . u . s . . .
p . a . . . . r . t . . . . . .
. . . e . z . . . . . d . . e .
. . . . . . m . a . . . . i . n

---

p v a e o z m r a t u d s i e n

Cette méthode qui paraît devoir donner naissance à des combinaisons nouvelles, est applicable à toutes les formes de grille.

Soit, pour exemple, une grille triangulaire, dont les fenêtres sont indiquées par o ; les vides des bandes le seront par un point.

. o . o . o

. o . . .

. . o .

o . .

. o

.

1re position. × . × . × . × . × × × × × . × . × × × . ×

2e — × × . × × × . × × . . × . × × × × . × × .

3e — . × × × . × × × . × × . × × . × . × . × ×

Il ne reste plus qu'à remplacer les points par les lettres de la dépêche et à faire le relèvement.

Nous n'avons, jusqu'ici, étudié les grilles qu'au point de vue de la transposition des lettres, ce sont les *grilles transposantes*, mais là ne se borne pas leur emploi, ainsi que nous le verrons en traitant des *grilles chiffrantes* et des *grilles transposantes et chiffrantes*.

Méthodes diverses. — De nombreux systèmes de transposition ont été inventés et il est facile d'en imaginer d'autres. Le but à atteindre est de modifier ou bouleverser l'ordre de succession, autrement dit la *séquence*, des lettres du texte, d'une manière méthodique permettant aux initiés de rétablir l'ordre primitif. Indépendamment des méthodes déjà exposées, on a proposé l'emploi des jeux de cartes, du taquin, etc., et de diverses combinaisons plus ou moins ingénieuses.

Les plus connues sont : la méthode du *Télégraphe aérien* et les *deux de M. le colonel Roche*, exposées toutes trois par M. le capitaine Josse dans sa brochure intitulée : *La Cryptographie et ses applications à l'art militaire*.

Méthode du Télégraphe aérien. — Cette méthode, imaginée pour correspondre secrètement par le télégraphe Chappe, peut être employée avec une combinaison de deux, trois, quatre, etc., lettres ou chiffres.

Pour s'en servir, on prépare un tableau contenant autant de colonnes qu'il entre de signes dans la combinaison. En marge,

on écrit, dans un ordre convenu, toutes les permutations que peuvent former les signes adoptés, en n'inscrivant qu'une seule permutation sur chaque ligne.

Soit 3142, la permutation de la première ligne; on portera la première lettre du *clair* dans la troisième colonne, indiquée par le chiffre 3 (premier de la permutation); la deuxième lettre claire sera posée dans la première colonne, indiquée par le chiffre 1 (deuxième de la permutation); la troisième claire occupera la quatrième colonne et la quatrième ira à la deuxième colonne. On opérera de même pour la deuxième ligne, en se guidant sur les chiffres de la deuxième permutation; quand toutes les lignes auront reçu leurs quatre lettres, on reviendra à la première, en opérant toujours de la même façon jusqu'à la fin du texte; on fera ensuite le relèvement suivant une méthode convenue.

Première méthode de M. le colonel Roche. — Cette ingénieuse méthode, qui mélange parfaitement les lettres, est entachée d'un défaut signalé par M. le capitaine Valério *(De la Cryptographie. — Essai sur les méthodes de déchiffrement)*. Ce défaut sera absolument évité en opérant de la manière suivante :

Choisir une série numérique très longue, sinon indéfinie. Les opérations arithmétiques, surtout les extractions de racines et les fractions irréductibles, nous fourniront, sous une forme condensée et facile à retenir, les éléments de ces séries. Ainsi la fraction 1/7, convertie en décimales, donnera une série de *six* chiffres : 1/7 = 0,142857... ; 1/49 donnera quarante-deux chiffres, etc. Supposons qu'on ait choisi 1/19 = 0,052631578947368421....

Marquons sur une ligne autant de points que la dépêche contient de lettres; séparons cette ligne en compartiments renfermant chacun le nombre de points indiqué par les chiffres significatifs de la série choisie.

Soit, par exemple, trente-trois le nombre des lettres du texte, nous aurons :

5	2	6	3	1	5	7	4
. . . . .	. .	. . . . . .	. . .	.	. . . . .	. . . .	. . . .

le dernier compartiment, qui ne renferme que quatre points, en aurait reçu huit si la dépêche avait eu trente-sept lettres ou plus.

On commencera par mettre dans chaque compartiment une des premières lettres du texte à cryptographier, en suivant l'ordre naturel de gauche à droite, ou un ordre arbitraire convenu à l'avance.

Supposons que l'on suive l'ordre naturel et que les huit premières lettres soient placées à la droite dans chaque compartiment; les lettres suivantes du texte seront mises, s'il est pos-

sible, à la droite de chacune des huit premières, en allant de gauche à droite ; dans le cas actuel, on n'en peut placer que six. A partir de la quinzième, les lettres claires seront posées à la gauche des lettres ou groupes déjà inscrits, en allant de droite à gauche ; on reprendra ensuite la marche de gauche à droite et ainsi de suite alternativement.

Cette opération fournira le tableau ci-dessous :

33.32.28.20.1 | 9.2 | 10.21.29.27.19.3 | 11.18.4 | 5 | 12.22.26.17.6 |
13.23.30.31.25.16.7 | 14.24.15.8

La **deuxième méthode de M. le colonel Roche** donne des résultats analogues à ceux de la première, dont elle n'est, du reste, qu'une modification consistant principalement dans la suppression de la série numérique, rendue inutile par l'introduction d'un nombre uniforme de lettres dans chaque compartiment.

Nous arrêtons ici l'étude des méthodes d'inversion. Les particularités de la langue permettant, le plus souvent, de rétablir le texte exact des dépêches cryptographiées avec les meilleures méthodes, surtout quand ces dépêches sont assez courtes pour que le nombre des tâtonnements à effectuer soit peu considérable.

Cependant, appliquées à un texte déjà chiffré *par d'autres méthodes*, les systèmes d'inversion peuvent rendre de réels services. Nous soulignons *par d'autres méthodes*, car ce serait une erreur de croire que l'emploi successif, sur un même texte, de plusieurs méthodes de transposition augmente les garanties de secret. La plupart du temps, il n'en est rien et les difficultés, tant du chiffrement que de la lecture, s'accroissent beaucoup plus rapidement que celles du déchiffrement sans clé.

DEUXIÈME PARTIE

SUBSTITUTION

La *substitution* consiste à remplacer les lettres du clair par des signes conventionnels, par des nombres ou par d'autres lettres.

L'emploi de signes conventionnels ne se prêtant pas aux communications télégraphiques, ce système n'est plus utilisé que très exceptionnellement. D'ailleurs, au point de vue du secret, la garantie est identiquement la même, le déchiffreur, attribuant à chaque signe un nombre ou une lettre, transforme les cryptogrammes de ce genre en cryptogrammes littéraux ou numériques, ce qui rend son travail plus facile, en lui permettant d'opérer sur des signes usuels.

La substitution est *simple* ou *complexe*.

On l'appelle *simple* ou *par monogrammes* lorsque chaque lettre du clair détermine une lettre du chiffre et réciproquement.

La substitution est *complexe* ou *par polygrammes* quand plusieurs lettres du clair entrent dans la détermination de *chacune* des lettres du chiffre et réciproquement, *indépendamment de toute clé*.

Nous nous occuperons, dans la deuxième partie, seulement de la substitution simple ou monogrammatique et nous consacrerons la troisième partie à la substitution complexe ou polygrammatique.

SUBSTITUTION SIMPLE

Monogrammes. — Systèmes alphabétiques.

Les systèmes de cette catégorie sont caractérisés par ce fait que chaque lettre du clair est remplacée par un signe, toujours le même pour une convention donnée.

Ils sont *monoalphabétiques* ou *polyalphabétiques*.

Nous les disons *monoalphabétiques*, lorsque la substitution se fait à l'aide d'un *seul* alphabet et polyalphabétiques, lorsque *plusieurs* alphabets *différents* sont employés au chiffrement.

La *clé* sert à indiquer le *point de départ* de l'alphabet employé, c'est donc la lettre ou le nombre de cet alphabet qui correspond à la lettre A.

La clé est *simple*, quand la même lettre, ou le même nombre, sert à opérer la transformation de toutes les lettres à cryptographier.

Elle est *multiple*, quand plusieurs lettres ou nombres servent à cette transformation.

La clé multiple est dite *périodique*, lorsqu'elle se reproduit indéfiniment et régulièrement sur toute la longueur du texte ; elle est dite *variable*, lorsque ses répétitions sont *tronquées* ou rendues *irrégulières* par une convention quelconque.

Système monoalphabétique. — Le système *monoalphabétique à clé simple* est connu sous le nom de *méthode de Jules César*, bien que ce système fort ancien eût déjà été employé, longtemps auparavant, par les Phéniciens et les Carthaginois : l'empereur Auguste s'en servait également pour écrire à ses enfants.

Au dire de Suétone et d'Aulu-Gelle, César se servait, pour correspondre secrètement avec ses amis, d'un alphabet où chaque lettre était avancée de quatre rangs.

Pour bien comprendre ce qui va suivre et voir clairement la liaison des diverses méthodes monogrammatiques, commençons par préparer des *bandes alphabétiques*.

Bandes alphabétiques. – Ces bandes seront constituées par d'étroites planchettes ou des rubans, soit de métal, soit de carton, sur lesquels nous inscrirons verticalement, dans leur ordre normal et à intervalles égaux, toutes les lettres de

l'alphabet usuel. — Il est utile d'écrire sur chaque bande *deux* alphabets semblables à la suite l'un de l'autre.

Posons nos bandes côte à côte et faisons-les glisser de manière à amener sur une même ligne horizontale les lettres formant le texte à chiffrer. Nous prendrons ensuite pour cryptogramme la ligne désignée par la clé, soit celle qui suit immédiatement le clair, si la clé est B, soit la deuxième avec la clé C, la troisième avec D, etc.

o	l	j	b	x	k	q	f	n	r	b
p	m	k	c	y	l	r	g	o	s	c
q	n	l	d	z	m	s	h	p	t	d
R	O	M	E	A	N	T	I	Q	U	E
s	p	n	f	b	o	u	j	r	v	f
t	q	o	g	c	p	v	k	s	w	g
u	r	p	h	d	q	w	l	t	x	h
v	s	q	i	e	r	x	m	u	y	i
w	t	r	j	f	s	y	n	v	z	j

Si la clé est simple, c'est-à-dire la même pour toutes les lettres du texte, notre cryptogramme sera :

Avec la clé B : *s p n f b o u j r v f*
— D : *u r p h d q w l t x h*
— Y : *p m k c y l r g o s c*, etc.

Obturateurs simples. — Afin de faciliter la lecture du cryptogramme, on peut se servir d'une bande de papier ou de carton à côtés parallèles et de largeur suffisante pour recouvrir ou masquer les lignes comprises entre le clair et le cryptogramme.

Si la clé est multiple, c'est-à-dire formée de plusieurs lettres, la bande obturante, rectiligne d'un côté, est, de l'autre, taillée en escalier, de telle sorte qu'elle recouvre un nombre inégal de lignes, selon les indications de la convention représentées par les lettres de la clé.

Soit D E C la clé convenue, c'est-à-dire le cryptogramme de A A A : toute lettre cryptographiée avec la clé D sera représentée par celle qui est placée trois rangs plus loin dans l'alphabet normal, puisque D occupe le troisième rang après A ; E occupant

le quatrième rang après A, toute lettre chiffrée avec la clé E sera représentée par celle qui la suit à quatre rangs de distance dans l'alphabet normal ; enfin C étant au deuxième rang après A, toutes les lettres cryptographiées avec C auront pour chiffres celles qui les suivent à deux rangs de distance dans l'alphabet normal.

L'obturateur devra donc être découpé de manière à masquer deux lettres pour la clé D, trois pour E et une pour C ; il prendra, par suite, la forme indiquée ci-dessous :

q	n	l	d	z	m	s	h	p	t	d	
R	O	M	E	A	N	T	I	Q	U	E	
»	»	»	»	»	»	»	»	»	»	»	»
»	»	o	»	»	p	»	»	s	»	»	
u	»	p	h	»	q	w	»	t	x	»	
v	s	q	i	e	r	x	m	u	y	i	
w	t	r	j	f	s	y	n	v	z	j	

et on aura pour cryptogramme : *usohepwmsxi*. En changeant l'obturateur de face, les lettres-chiffres se trouvent en ligne droite et les claires suivent la ligne brisée, ce qui est peut-être plus commode pour la traduction.

Obturateurs doubles. — Un obturateur en escalier d'une certaine longueur, ne laissant pas d'être d'un maniement difficile et nécessitant de nombreuses bandes alphabétiques, on est conduit à se demander s'il n'est pas préférable d'employer successivement deux obturateurs. Cette solution doit être rejetée, car elle double le travail du chiffrement et celui de la traduction et augmente, en outre, considérablement les chances d'erreurs, toutes choses qu'il convient d'éviter.

Nos recherches, dans cet ordre d'idées, nous ont conduit à l'*obturateur double*, qui est d'un maniement assez facile et n'exige qu'un très petit nombre de bandes alphabétiques et qui fournit une clé d'une longueur considérable.

Imaginons que par un moyen quelconque, par exemple une mince coulisse métallique, on puisse réunir les côtés rectilignes de deux obturateurs et les faire glisser l'un sur l'autre, on obtiendra ainsi un obturateur à deux escaliers.

Découpons, dans de fort papier quadrillé, un obturateur A masquant une lettre de la première bande alphabétique, quatre de la deuxième et deux de la troisième, soit $A = 142$; formons un second obturateur $B = 23154$; A agissant sur trois alphabets, B sur cinq, et les nombres 3 et 5 étant premiers entre eux, en faisant glisser A sur B, on obtiendra une période de $3 \times 5 = 15$:

$$A_1 = 1\ 4\ 2.1\ 4\ 2.1\ 4\ 2.1\ 4\ 2.1\ 4\ 2.$$
$$B_1 = 2\ 3\ 1\ 5\ 4.2\ 3\ 1\ 5\ 4.2\ 3\ 1\ 5\ 4.$$
$$A_1 + B_1 = 3\ 7\ 3\ 6\ 8\ 4\ 4\ 5\ 7\ 5\ 6\ 5\ 2\ 9\ 6.$$

Si maintenant nous renversons un des obturateurs simples, A, par exemple, nous aurons $A_2 = 241$ et :

$$A_2 = 2\ 4\ 1.2\ 4\ 1.2\ 4\ 1.2\ 4\ 1.2\ 4\ 1.$$
$$B_1 = 2\ 3\ 1\ 5\ 4.2\ 3\ 1\ 5\ 4.2\ 3\ 1\ 5\ 4.$$
$$A_2 + B_1 = 4\ 7\ 2\ 7\ 8\ 3\ 5\ 5\ 6\ 6\ 6\ 4\ 3\ 9\ 5.$$

Nous obtenons ainsi deux périodes de quinze chiffres ou une clé de $2 \times 15 = 30$ caractères; nous arrivons au double, $2 \times 30 = 60$, en renversant, à son tour, l'autre obturateur, qui devient $B_2 = 45132$:

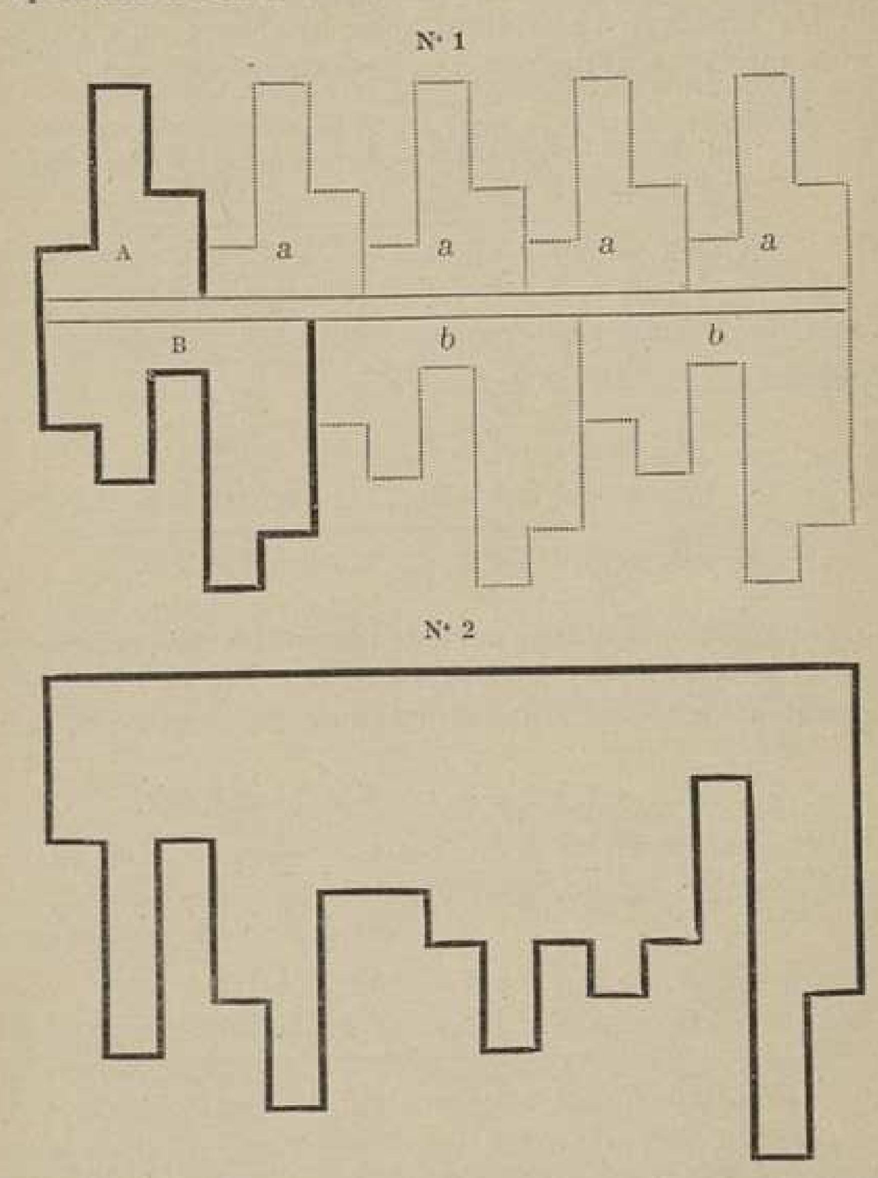
$$A_1 = 1\ 4\ 2.1\ 4\ 2.1\ 4\ 2.1\ 4\ 2.1\ 4\ 2.$$
$$B_2 = 4\ 5\ 1\ 3\ 2.4\ 5\ 1\ 3\ 2.4\ 5\ 1\ 3\ 2.$$
$$A_1 + B_2 = 5\ 9\ 3\ 4\ 6\ 6\ 6\ 5\ 5\ 3\ 8\ 7\ 2\ 7\ 4.$$

$$A_2 = 2\ 4\ 1.2\ 4\ 1.2\ 4\ 1.2\ 4\ 1.2\ 4\ 1.$$
$$B_2 = 4\ 5\ 1\ 3\ 2.4\ 5\ 1\ 3\ 2.4\ 5\ 1\ 3\ 2.$$
$$A_2 + B_2 = 6\ 9\ 2\ 5\ 6\ 5\ 7\ 5\ 4\ 4\ 8\ 6\ 3\ 7\ 3.$$

Enfin, si après avoir cryptographié en plaçant l'obturateur en *dessous* du texte clair, nous le posons en *dessus*, nous doublons le nombre des caractères de la clé, que nous portons à $2 \times 60 = 120$ et trois bandes alphabétiques, cinq au plus, suffisent pour ce travail.

Note. — L'emploi des alphabets intervertis, dont nous ne tarderons pas à nous occuper, porterait le nombre des caractères de la clé à $3 \times 120 = 360$, ou à $5 \times 120 = 600$, par le simple roulement des alphabets, suivant le système indiqué à la page 65; en faisant usage de toutes les permutations possibles, les nombres ci-dessus deviendraient, pour trois alphabets : $6 \times 120 = 720$, et pour cinq alphabets : $120 \times 120 = 14.400$.

Ci-dessous, un diagramme représentant l'obturateur double A,+B, et indiquant les diverses positions des obturateurs simples A, B ; la deuxième figure montre l'obturateur à un côté rectiligne correspondant à l'obturateur double :



Chiffre de Vigenère.—Juxtaposons vingt-six bandes, en amenant, sur la première ligne et dans l'ordre normal, toutes les lettres de l'alphabet usuel, et nous obtiendrons le tableau imaginé, vers la fin du XVIe siècle, par le diplomate français Blaise de Vigenère (1523-1596).

Ce tableau porte le nom de *chiffre carré* et celui de *chiffre indéchiffrable* ou *chiffre par excellence*. Il a été fort employé dans les chancelleries aux XVIIe et XVIIIe siècles et sert encore de base à un grand nombre de systèmes contemporains, qui n'en sont, pour la plupart, que des modifications plus ou moins ingénieuses.

Les lignes de ce tableau peuvent être considérées comme des

alphabets nouveaux, mais il est facile de reconnaître que ce n'est que l'alphabet normal, dont les lettres sont reculées de 1, 2, 3... 25 rangs. Nous les désignerons par la dénomination de *sous-alphabets*.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Pour cryptographier avec ce tableau, on divise le texte clair en groupes renfermant autant de lettres qu'il y en a à la clé; puis on écrit la clé sous chaque groupe, en la répétant autant que de besoin. On inscrit ensuite, sur une troisième ligne, la lettre qui se trouve dans le tableau à l'intersection de la colonne commençant par la lettre à cryptographier et de la rangée débutant par la lettre de la clé.

Soit, comme exemple, les mots chiffrés plus haut avec la clé DEC :

r o m	e a n	t i q	u e
D E C	D E C	D E C	D E
u s o	h e p	w m s	x i

Nous obtenons le même cryptogramme que par la méthode précédente.

C'est aussi le chiffre de DEC cryptographié avec les polygrammes : *rom*, *ean*, *tiq*, *ue*, pris successivement pour clés.

Ce résultat est dû à la parfaite symétrie des sous-alphabets, qui sont constitués horizontalement et verticalement suivant la même loi.

Dans la pratique, on trouve plus facile de chiffrer en même temps toutes les lettres qui, occupant le même rang dans les groupes, ressortissent au même sous-alphabet et sont accompagnées de la même lettre-clé. Quand le nombre des lettres de la clé est assez considérable, il est encore plus commode d'écrire les lettres du clair en colonnes surmontées chacune de la lettre-clé convenable et alors on chiffre toutes les lettres d'une colonne avant de s'occuper de la suivante, ce qui réduit considérablement le travail en facilitant les recherches sur le tableau, puisque la même ligne sert au chiffrement de toute une colonne.

De l'emploi de l'alphabet normal pour la formation du chiffre carré résulte un inconvénient particulièrement grave. Il suffit, en effet, que le déchiffreur parvienne à reconnaitre la valeur exacte d'une *seule* lettre pour que le sous-alphabet auquel elle appartient soit complètement connu.

Alphabets intervertis. — Pour obvier à cet inconvénient, on intervertit l'alphabet normal en changeant l'ordre de succession des lettres. On peut, à cet effet, prendre un mot ou une phrase facile à retenir. Soit le mot géographique *Klagenfurth*, choisi pour exemple par M. Josse. On écrit, à la suite de ce mot, dans leur ordre alphabétique, toutes les lettres qu'il ne renferme pas, et l'alphabet est formé.

Rapprochons cette suite de lettres de l'alphabet normal :

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
k	*l*	*a*	*g*	*e*	*n*	*f*	*u*	*r*	*t*	*h*	*b*	*c*	*d*	*i*	*j*	*m*	*o*	*p*	*q*	*s*	*v*	*w*	*x*	*y*	*z*

et nous verrons que A étant représenté par K, B par L, C par A, etc., la connaissance d'une ou de plusieurs lettres n'entraine plus la connaissance des autres pour les personnes qui ignorent le mot servant de base au nouvel alphabet.

On chiffre en substituant aux lettres claires, lues sur la première ligne, celles qui leur correspondent sur la seconde, ainsi :

L A C R Y P T O G R A P H I E
devient : *b k a o y j q i f o k j u r e.*

La lecture se fait en cherchant les lettres du cryptogramme

sur la seconde ligne et en les remplaçant par celles de la première.

On pourrait aussi classer *normalement* les lettres de la deuxième ligne, ce qui fournirait l'alphabet :

C L M N E G D K O P A B Q F R S T I U J H V W X Y Z
a b c d e f g h i j k l m n o p q r s t u v w x y z

Chacun de ces alphabets est dit *déchiffrant* par rapport à l'autre pris comme type ou alphabet *chiffrant*.

Chiffre carré à alphabet interverti régulièrement. — Tout alphabet *interverti* peut servir de base pour la formation d'un chiffre carré, auquel on donne habituellement, à tort, la disposition suivante :

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	k	l	a	g	e	n	f	u	r	t	h	b	c	d	i	j	m	o	p	q	s	v	w	x	y	z
B	l	a	g	e	n	f	u	r	t	h	b	c	d	i	j	m	o	p	q	s	v	w	x	y	z	k
C	a	g	e	n	f	u	r	t	h	b	c	d	i	j	m	o	p	q	s	v	w	x	y	z	k	l
D	g	e	n	f	u	r	t	h	b	c	d	i	j	m	o	p	q	s	v	w	x	y	z	k	l	a
E	e	n	f	u	r	t	h	b	c	d	i	j	m	o	p	q	s	v	w	x	y	z	k	l	a	g
F	n	f	u	r	t	h	b	c	d	i	j	m	o	p	q	s	v	w	x	y	z	k	l	a	g	e
G	f	u	r	t	h	b	c	d	i	j	m	o	p	q	s	v	w	x	y	z	k	l	a	g	e	n
H	u	r	t	h	b	c	d	i	j	m	o	p	q	s	v	w	x	y	z	k	l	a	g	e	n	f
I	r	t	h	b	c	d	i	j	m	o	p	q	s	v	w	x	y	z	k	l	a	g	e	n	f	u
J	t	h	b	c	d	i	j	m	o	p	q	s	v	w	x	y	z	k	l	a	g	e	n	f	u	r
K	h	b	c	d	i	j	m	o	p	q	s	v	w	x	y	z	k	l	a	g	e	n	f	u	r	t
L	b	c	d	i	j	m	o	p	q	s	v	w	x	y	z	k	l	a	g	e	n	f	u	r	t	h
M	c	d	i	j	m	o	p	q	s	v	w	x	y	z	k	l	a	g	e	n	f	u	r	t	h	b
N	d	i	j	m	o	p	q	s	v	w	x	y	z	k	l	a	g	e	n	f	u	r	t	h	b	c
O	i	j	m	o	p	q	s	v	w	x	y	z	k	l	a	g	e	n	f	u	r	t	h	b	c	d
P	j	m	o	p	q	s	v	w	x	y	z	k	l	a	g	e	n	f	u	r	t	h	b	c	d	i
Q	m	o	p	q	s	v	w	x	y	z	k	l	a	g	e	n	f	u	r	t	h	b	c	d	i	j
R	o	p	q	s	v	w	x	y	z	k	l	a	g	e	n	f	u	r	t	h	b	c	d	i	j	m
S	p	q	s	v	w	x	y	z	k	l	a	g	e	n	f	u	r	t	h	b	c	d	i	j	m	o
T	q	s	v	w	x	y	z	k	l	a	g	e	n	f	u	r	t	h	b	c	d	i	j	m	o	p
U	s	v	w	x	y	z	k	l	a	g	e	n	f	u	r	t	h	b	c	d	i	j	m	o	p	q
V	v	w	x	y	z	k	l	a	g	e	n	f	u	r	t	h	b	c	d	i	j	m	o	p	q	s
W	w	x	y	z	k	l	a	g	e	n	f	u	r	t	h	b	c	d	i	j	m	o	p	q	s	v
X	x	y	z	k	l	a	g	e	n	f	u	r	t	h	b	c	d	i	j	m	o	p	q	s	v	w
Y	y	z	k	l	a	g	e	n	f	u	r	t	h	b	c	d	i	j	m	o	p	q	s	v	w	x
Z	z	k	l	a	g	e	n	f	u	r	t	h	b	c	d	i	j	m	o	p	q	s	v	w	x	y

On se sert de ce tableau comme de celui de Vigenère. Prenant la lettre claire à cryptographier dans l'alphabet normal qui borde horizontalement le tableau, on descend verticalement la colonne qu'elle surmonte jusqu'au sous-alphabet précisé par la lettre-clé, et l'on prend pour chiffre la lettre appartenant, à la fois, à la colonne de la lettre claire et au sous-alphabet choisi. Par suite de la double symétrie du tableau, on peut prendre la lettre claire dans l'alphabet normal qui borde verticalement la gauche du tableau et alors le sous-alphabet à employer est spécifié par l'une des lettres de l'alphabet normal horizontal.

Soit, par exemple, à chiffrer, avec la clé : MATIN, la phrase : *Venez me voir de suite,* on opère comme l'indique le diagramme :

v e n e z	m e v o i	r d e s u	i t e
M A T I N	M A T I N	M A T I N	M A T
u e f c c	y e i w v	g g x k u	s q x

et on aura : *Venez me voir de suite = uefccyeiwvggxkusqx.*

Pour traduire en clair, on opère d'une manière inverse, c'est-à-dire que, après avoir, dans le cas actuel, partagé le texte chiffré en groupes de cinq lettres, on cherche la première lettre de chacun de ces groupes dans le sous-alphabet M et on écrit au-dessous celles qui leur correspondent verticalement dans l'alphabet normal horizontal.

On cherche ensuite la deuxième lettre de chaque groupe dans le sous-alphabet A, la troisième dans le sous-alphabet T, et on les remplace par leurs correspondantes de l'alphabet normal supérieur.

Symétrie de position. — Bien que dans les chiffres carrés ayant un alphabet interverti pour base, on ne puisse plus déduire un sous-alphabet entier de la connaissance d'une seule lettre, la symétrie horizontale, comme l'a démontré M. Kerckhoffs dans sa *Cryptographie militaire,* fournit au déchiffreur un remarquable moyen d'abréger les tâtonnements et de reconstituer le chiffre inconnu qu'il recherche.

En effet, un sous-alphabet n'est que l'alphabet principal dont le point de départ est changé, puisque la suite des lettres restant invariable, l'*origine,* c'est-à-dire la lettre qui représente A, varie de la première à la dernière lettre de l'alphabet, sans que l'ordre de ces lettres soit modifié. Il en résulte que, dans tous les sous-alphabets, le même intervalle sépare deux lettres déterminées, de telle sorte que, dès que la signification d'un chiffre a été trouvée dans plusieurs sous-alphabets, une simple addition suffit pour déterminer la *place* que doit occuper, dans ces sous-alpha-

bets, tout nouveau chiffre dont la valeur serait établie pour un seul.

Prenons un exemple : Supposons que ses premiers tâtonnements sur un cryptogramme ait amené un déchiffreur à reconnaître la valeur des chiffres attribués aux voyelles dans quatre sous-alphabets ; s'il remarque que ces sous-alphabets sont reliés par les trois chiffres POI appartenant : P aux premier et deuxième, O aux deuxième et troisième et I aux troisième et quatrième, il lui suffira pour reconstituer l'alphabet principal de reporter tous les chiffres connus sur une seule ligne en maintenant les intervalles qui séparent chaque chiffre de la lettre commune, comme l'indique le diagramme suivant :

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	X	Y	Z
1er	P	.	.	.	e	.	.	.	l	.	.	.	.	.	h	.	.	.	.	.	u	.	.	y	.
2e	O	.	.	.	t	.	.	.	b	.	.	.	.	.	m	.	.	.	.		x	.	.	P	
3e	I	.	.	.	d	.	.	.	k	.	.	.	.	.	v	.	.	.	.	.	O	.	.	c	.
4e	z	.	.	.	j	.	.	.	I	.	.	.	.	.	g	.	.	.	.	.	s	.	.	.	.

P	.	o	j	e	c	t	i	l	.	b	d	.	g	h	k	m	.	.	s	u	v	x	y	z

Il est inutile de faire remarquer qu'au cours de ce travail on est conduit à reconnaître que l'alphabet cherché n'a que vingt-cinq lettres.

Nous verrons plus loin le moyen d'éviter cette *symétrie de position*, comme l'appelle M. Kerckhoffs, qui met une arme redoutable entre les mains de l'ennemi, c'est-à-dire du déchiffreur sans clé.

Alphabets à lettres couplées. — Ce système de cryptographie, fort ancien puisqu'on en trouve des traces dans la Bible, consiste à replier l'alphabet usuel sur lui-même et à substituer à chaque lettre claire la lettre qui lui correspond dans l'autre moitié de l'alphabet.

Soit : A B C D E F G H I J K L M
Z Y X W V U T S R Q P O N

Pour cryptographier PARIS, nous écrirons KZIRH, en remplaçant P par K, A par Z, R par I, et réciproquement, I par R, et enfin S par H.

Système de Porta. — Le système du physicien Porta (1540-1615) est basé sur cet arrangement, mais il fournit le moyen de faire varier la clé.

Il consiste essentiellement à écrire, sous le demi-alphabet normal (A à M) le reste de l'alphabet, dont on fait varier les lettres comme dans le tableau de Vigenère :

Clés	A	B	C	D	E	F	G	H	I	J	K	L	M
A.N	n	o	p	q	r	s	t	u	v	w	x	y	z
B.Z	z	n	o	p	q	r	s	t	u	v	w	x	y
C.Y	y	z	n	o	p	q	r	s	t	u	v	w	x
D.X	x	y	z	n	o	p	q	r	s	t	u	v	w
E.W	w	x	y	z	n	o	p	q	r	s	t	u	v
F.V	v	w	x	y	z	n	o	p	q	r	s	t	u
G.U	u	v	w	x	y	z	n	o	p	q	r	s	t
H.T	t	u	v	w	x	y	z	n	o	p	q	r	s
I.S	s	t	u	v	w	x	y	z	n	o	p	q	r
J.R	r	s	t	u	v	w	x	y	z	n	o	p	q
K.Q	q	r	s	t	u	v	w	x	y	z	n	o	p
L.P	p	q	r	s	t	u	v	w	x	y	z	n	o
M.O	o	p	q	r	s	t	u	v	w	x	y	z	n

Pour faire usage de ce tableau, il faut, si la lettre à cryptographier est comprise entre A et M, la chercher à la ligne supérieure, descendre la colonne verticale jusqu'à la rangée précisée par la clé choisie et prendre pour chiffre la lettre qui se trouve à l'intersection. Faire l'inverse, si la lettre à cryptographier appartient à la seconde moitié de l'alphabet normal, c'est-à-dire suivre la rangée horizontale indiquée par la clé jusqu'à la rencontre de la lettre à cryptographier et prendre pour chiffre la lettre du demi-alphabet qui se trouve placée immédiatement au-dessus.

Exemple : traduire, avec la clé : BON, la phrase : *sa dépêche est arrivée.*

s	a	d	e	p	e	c	h	e	e	s	t	a	r	r	i	v	e	e
B	O	N	B	O	N	B	O	N	B	O	N	B	O	N	B	O	N	B
g	o	q	q	b	r	o	v	r	q	e	g	z	d	e	u	h	r	q

On remarque que, dans le troisième alphabet (clé : N), *e* se traduit par *r* et, réciproquement, *r* par *e*. Il en est de même de toutes les lettres qui sont liées deux à deux, ce qui facilite beaucoup les tâtonnements. Du reste, comme dans le chiffre carré de Vigenère, dont celui-ci n'est qu'un abrégé, la détermination d'un

seul chiffre entraîne la connaissance de tout le sous-alphabet.

La traduction se fait identiquement comme le chiffrement.

Afin de faciliter l'emploi d'un mot-clé, les lettres servant à désigner chaque alphabet ont été doublées : l'une représente le chiffre de A, première lettre de l'un des demi-alphabets, et l'autre le chiffre de N première lettre du second demi-alphabet.

Méthode anglaise ou de Beaufort. — L'amiral anglais, sir Francis Beaufort a imaginé, en 1857, un nouvel emploi du tableau de Vigenère.

Ce tableau est complété par le report, sur la droite, de la première colonne de gauche et, au bas de la première rangée horizontale, de telle sorte que le chiffre carré est encadré par l'alphabet normal, écrit horizontalement de gauche à droite et verticalement de haut en bas.

Pour chiffrer, partant de la lettre claire, prise sur l'un quelconque des alphabets en bordure, on suit la colonne ou la rangée jusqu'à la lettre-clé, puis tournant à angle droit, on prend pour chiffre la lettre qui termine la nouvelle ligne, horizontale ou verticale, suivie depuis la lettre-clé.

M. Kerckhoffs a démontré que les cryptogrammes obtenus par la méthode de Beaufort étaient identiques avec ceux fournis par le système de Vigenère, en retournant simplement l'alphabet normal ; mais il a omis de dire que cette méthode n'est qu'une modification heureuse de celle de Porta, les lettres de chaque sous-alphabet étant couplées, toute lettre qui sert de chiffre à une autre est, à son tour, chiffrée par celle-ci. On peut donc, au lieu d'écrire le chiffre carré de la manière habituelle, donner aux alphabets la disposition indiquée ci-dessous, qui en facilite l'emploi :

A	A	B	C	D	E	F	G	H	I	J	K	L	M	N
	a	z	y	x	w	v	u	t	s	r	q	p	o	n
B	B	C	D	E	F	G	H	I	J	K	L	M	N	
	a	z	y	x	w	v	u	t	s	r	q	p	o	
C	B	C	D	E	F	G	H	I	J	K	L	M	N	O
	b	a	z	y	x	w	v	u	t	s	r	q	p	o
D	C	D	E	F	G	H	I	J	K	L	M	N	O	
	b	a	z	y	x	w	v	u	t	s	r	q	p	
E	C	D	E	F	G	H	I	J	K	L	M	N	O	P
	c	b	a	z	y	x	w	v	u	t	s	r	q	p

. . . .

. . . .

Le diagramme ci-après donne le détail du chiffrement du texte clair : *Préparez-vous à lever le camp*, avec la clé : HONNEUR ET PATRIE.

p	r	e	p	a	r	e	z	v	o	u	s	a	l	e	v	e	r	l	e	c	a	m	p
H	O	N	N	E	U	R	E	T	P	A	T	R	I	E	H	O	N	N	E	U	R	E	T
s	x	j	y	e	d	n	f	y	b	g	b	r	x	a	m	k	w	c	a	s	r	s	e

On a pour cryptogramme :

sxjyednfybgbrxamkwcasrse

Systèmes numériques. — Nous commencerons l'étude de ces systèmes par la *méthode de Gronsfeld.*

Cette méthode consiste à prendre pour clé des nombres faciles à retenir. Ces nombres sont écrits sous les lettres du texte clair et répétés autant de fois qu'il est nécessaire. On prend ensuite, pour représenter chaque lettre claire, celle qui se trouve placée dans l'alphabet normal à une distance égale au chiffre inscrit au-dessous, en comptant de A à Z.

Soit à cryptographier : *Détruisez les ponts*, avec la clé : 502.

D	e	t	r	u	i	s	e	z	l	e	s	p	o	n	t	s
5	0	2	5	0	2	5	0	2	5	0	2	5	0	2	5	0
i	e	v	w	u	k	x	e	b	q	e	u	u	o	p	y	s

Pour traduire, on effectue la même opération, mais en remontant l'alphabet.

En cryptographiant avec le même nombre la lettre A considérée comme origine de l'alphabet normal, nous trouverons le mot : FAC qui, pris comme clé, nous fournira, à l'aide du tableau de Vigenère, identiquement le même cryptogramme pour la dépêche ci-dessus.

Bien d'autres méthodes numériques ont été imaginées, mais, de même que la précédente, ce ne sont que des formes déguisées de la méthode de Vigenère, ainsi que nous aurons occasion de le constater pour les méthodes de MM. Auvray et Delauney.

Alphabet numérique. — Afin d'établir clairement les *équations cryptographiques*, il est utile de transformer l'alphabet littéral en *alphabet numérique*. Pour cela, attribuons à chaque lettre un nombre, celui qui indique sa distance à l'origine de l'alphabet, soit A pour l'alphabet normal ; nous aurons ainsi :

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

En prolongeant ce tableau, on trouvera, pour le 2[e] alphabet :

A	B	C	D	E	F	G	H	I	J	etc.
26	27	28	29	30	31	32	33	34	35	etc.

pour le 3[e] :

A	B	C	D	E	F	G	H	etc.
52	53	54	55	56	57	58	59	etc.

et, en général, pour le $n+1^{me}$:

A	B	C	D	etc.
$26n$	$26n+1$	$26n+2$	$26n+3$	

En d'autres termes, chaque lettre est spécifiée par son numéro minimum, pris dans le premier alphabet, et augmenté ou non d'un multiple de 26 ; ce multiple ne serait que de 25, si on n'introduisait pas le W dans l'alphabet : en rejetant une autre lettre, J ou V par exemple, on n'aurait à tenir compte que d'un multiple de 24, nombre des lettres de l'alphabet adopté.

Equations cryptographiques. — Les alphabets étant ainsi transformés en une suite de nombres en *progression arithmétique*, il est facile d'en déduire les formules que M. de Viaris a dénommées : *équations cryptographiques.*

Tous les systèmes de substitution alphabétiques, à l'exception de celui de Porta, qui est un peu plus compliqué, se réduisent à la solution du problème, dont la solution est bien connue :

Connaissant trois termes d'une proportion arithmétique, trouver le quatrième ?

Soit cryptographiquement : *Connaissant la valeur d'une lettre dans un sous-alphabet, trouver la valeur d'une autre lettre dans le même sous-alphabet ?*

Exemple : Sachant que, dans un sous-alphabet donné, D se traduit par H, par quelle lettre se traduira L ?

Dans l'alphabet numérique ci-dessus, $D = 3$, $H = 7$, $L = 11$. Arithmétiquement, nous devons avoir : $H - D = x - L$, ou $x = L + (H - D)$, en nombres : $x = 11 + (7 - 3) = 15$ ou P. Toutes les lettres de ce même sous-alphabet sont liées à leurs chiffres par la même relation : $x = l + 4$, en désignant par l une lettre quelconque et par x son cryptogramme.

Afin de simplifier l'énoncé des conventions, au lieu de déterminer un sous-alphabet par deux lettres, dont l'une est la valeur cryptographique de l'autre, on l'indique par une seule lettre, que l'on appelle *clé* et qui est le cryptogramme de la première lettre de l'alphabet adopté, soit A dans le cas de l'alphabet normal. La première lettre, ou *l'origine*, d'un alphabet ayant *zéro* pour valeur numérique, les équations ne nécessiteront que trois lettres au lieu de quatre.

En représentant l'origine par O, la clé par c, la lettre à crypto-

graphier par l et son chiffre par x, nous pouvons former les six proportions arithmétiques :

1er... $o.l:c.x.$ 2e.... $o.l:x\ c.$ 3e... $o\ c:x\ l.$
4e.... $o\ c:l.x.$ 5e.... $o.x:l\ c.$ 6e.... $o\ x:c.l.$

Appliquées à un même alphabet, ces six proportions ne fournissent que trois équations, les dernières reproduisant simplement les trois premières :

1er....... $x_1 = c + l$, système de Vigenère ;
2e......... $x_2 = c - l$, — de Beaufort ;
3e......... $x_3 = l - c$, — allemand.

Le système dénommé par M. Josse *méthode allemande* consiste à opérer pour le *chiffrement* comme on opère pour le *déchiffrement*, dans la méthode de Vigenère, et *vice versa*.

Dans cette méthode, la clé est employée *négativement*, ce qui nous amène à dire quelques mots au sujet des lettres-clés.

Modifications des lettres-clés. — L'emploi d'une clé négative n'étant pas commode dans la pratique, il est utile de la remplacer par sa *sous-clé*, qui n'est autre chose que son complément alphabétique. Nous savons, en effet, que chaque lettre est définie par un nombre *minimum* lequel, égal ou supérieur à zéro, est inférieur à 26 ou à 25, suivant l'alphabet adopté et que l'addition d'un multiple de 26 ou de 25, selon le cas, n'en change pas la valeur. Nous pouvons, dès lors, au lieu de zéro, attribuer à l'*origine* A la valeur de 26. En retranchant de ce nombre la valeur de la lettre-clé négative, on aura un nombre positif inférieur à 26 et représentant la lettre qui traduit A, soit une clé *positive*.

Chaque fois que nous aurons affaire à une clé négative, nous pourrons donc lui substituer son complément en faisant : $c' = 26 - c$.

Il résulte de ce qui précède que l'équation (3) se confond avec (1) et qu'il n'existe, par suite, que deux équations cryptographiques : l'une s'appliquant au système de Vigenère et l'autre à celui de Beaufort.

Il convient de faire remarquer que, des trois quantités entrant dans chacune de ces équations, l'une est fixe, c, et les deux autres variables, l et c. Toute nouvelle quantité *fixe* introduite dans ces formules aura donc pour effet de modifier l'apparence de la clé et, selon son application, de transformer, souvent à l'insu même du chiffreur, les équations l'une pour l'autre.

Ainsi M. de Viaris, dans sa *Cryptographie*, voulant augmenter les garanties de secret de la formule de Vigenère : $x = c + l$,

propose de retrancher les cryptogrammes ainsi obtenus d'un nombre fixé par convention, c'est-à-dire de faire l'opération indiquée par la relation : $x' = n - x$. Il est évident que, en remplaçant dans cette dernière formule x par sa valeur prise dans la première, on aura : $x' = n - c - l$; n et c étant des nombres fixes, nous pouvons poser : $c' = n - c$ et l'équation définitive deviendra : $x' = c' - l$, qui appartient au système de Beaufort.

Il en est de même de la méthode de M. Auvray, exposée par M. Josse dans sa brochure déjà plusieurs fois mentionnée.

Méthode Auvray. — Cette méthode consiste essentiellement à numéroter les lettres de l'alphabet normal, en ajoutant à celles employées comme clés un augment facile à retenir de mémoire, tel que : 50, 100, 1.000, par exemple. On cryptographie en retranchant la valeur de chaque lettre claire de celle de la lettre-clé placée au-dessus. On obtient ainsi une série de nombres de deux ou trois chiffres d'une apparence indéchiffrable. Voici, du reste, un cryptogramme donné par M. Josse pour exemple :

92—97—109—98—104—103—113—79—98 - 101—80—101—117—97—100—86—110—96—102—100—118—117—92—104.

L'alphabet étant de vingt-six lettres, nous pouvons, sans modifier le cryptogramme, retrancher de chaque nombre le plus grand multiple de 26, qui y est contenu. Les résidus seront :

14—19—5—20-0—25—9—1—20—23—2—23—13—19—22—8—6—18—24—22—14—13—14-0.

Sachant que l'augment employé était : $100 = 4 \times 26 - 4$, nous ajouterons 4 à chacun de ces derniers nombres, et il viendra :

18—23—9—24—4—3—13—5—24—1—6—1—17—23—0—12—10—22—2—0—18—17—18-4, nombres qui, transformés en lettres à l'aide de l'alphabet numérique normal, donneront :

sxjyednfybgbrxamkwcasrse

soit le cryptogramme que nous avons obtenu, à la page 42, en chiffrant, par la méthode de Beaufort, la même dépêche avec la même clé.

Nous avons vu que, en substituant, dans le tableau de Vigenère, un alphabet *interverti* à l'alphabet normal, les garanties de secret sont peu augmentées ; nous pouvons aussi reconnaître que le travail de traduction est beaucoup plus pénible, ce qui tient à la difficulté de retrouver, dans chaque sous-alphabet, les lettres dont on a besoin, alors que l'ordre normal n'est pas suivi. Cet inconvénient pourrait être évité par la formation d'un tableau déchiffrant, mais l'établissement des chiffres carrés est long et

pénible; en outre, leur conservation peut être dangereuse dans beaucoup de cas; il y a donc lieu de rechercher s'il n'existe pas un moyen pratique de supprimer les chiffres carrés et, tout en corrigeant les défauts signalés plus haut, de permettre l'application des équations cryptographiques.

Ce moyen est fourni par les bandes alphabétiques, généralisation du système dit de *Saint-Cyr*, mais la nouvelle méthode permettant de remplacer les *sous-alphabets* du chiffre carré par des *alphabets différents*, nous sortons des systèmes monoalphabétiques et il semble normal d'exposer les divers modes d'*interversion* de l'alphabet avant d'entreprendre l'étude des systèmes polyalphabétiques.

Interversion de l'alphabet normal. — Il est évident que si nous considérons l'alphabet normal comme un texte clair à cryptographier, nous pouvons lui appliquer l'une quelconque des méthodes de transposition exposées plus haut : ordre tiré au sort, parallélogrammes et carrés avec leurs divers relèvements, grilles, etc.

La méthode le plus généralement adoptée consiste dans le choix d'un mot, dont on supprime les lettres répétées et à la suite duquel on inscrit, en suivant l'ordre normal, les lettres que ce mot ne contient pas.

Cette méthode est défectueuse en ce que les lettres sont insuffisamment mélangées, ainsi dans l'alphabet :

KLAGENFURTHBCDIJMOPQSVWXYZ

formé d'après ce principe, nous trouvons juxtaposées les lettres : B, C, D — I, J — O, P, Q — V, W, X, Y, Z. En outre, ces cinq dernières occupent leurs places normales, toutes circonstances dont un déchiffreur avisé ne manquerait pas de tirer parti.

On a essayé d'obvier à cet inconvénient en écrivant sur plusieurs lignes, en dessous du mot choisi, répétitions déduites, les lettres non encore employées et de relever le tout par colonne du haut en bas ou du bas en haut :

R	E	P	U	B	L	I	Q
a	c	d	f	g	h	j	k
m	n	o	s	t	v	x	y
z	.	.	.	.	.	.	.

donnera : RAMZECNPDOUFSBGTLHVIJXQKY.

Cette méthode, critiquée par M. de Viaris (*L'art de chiffrer et déchiffrer les dépêches secrètes*), à qui l'exemple ci-dessus a été emprunté, est susceptible de nombreuses variantes.

Nous ne citerons que les deux suivantes : la première consiste à écrire l'alphabet normal sous le mot-clé, dont les lettres classées alphabétiquement indiquent l'ordre à suivre dans le relèvement :

5	1	3	4	2	6
R	E	N	N	E	S
a	b	c	d	e	f
g	h	i	j	k	l
m	n	o	p	q	r
s	t	u	v	x	y
z	.	.	.	.	.

d'où l'alphabet : BHNTEKQXCIOUDJPVAGMSZFLRY.

Dans l'autre système, plus complet, on intervertit également lès lignes, d'après la même clé ou d'après une autre :

	3	1	4	2	5
2 —	P	A	R	I	S
4 —	b	c	d	e	f
1 —	g	h	j	k	l
3 —	m	n	o	q	t
5 —	u	v	x	y	z

soit, après double transposition et relèvement :

HANCVKIQEYGPMBUJRODXLSTFZ.

Divers auteurs ont publié des séries d'alphabets intervertis (M. de Viaris, 600 ; M. Krohn, 3,200 ; M. Grivel, 26,000, etc), mais ces collections ne peuvent avoir aucune utilité pratique, du moins pour le service d'une armée en campagne, où l'officier cryptographe doit toujours pouvoir, avec un crayon et du papier, reconstituer les documents dont il a besoin pour chiffrer et pour traduire et où la nécessité de faire usage d'un livre spécial pourrait présenter les plus graves inconvénients.

L'auteur du présent travail a cru trouver la solution de l'important problème de la formation des alphabets intervertis dans la *décimation*. (*Cryptographie nouvelle*, 1893.)

Décimation. — La décimation peut être *directe* ou *inverse*.

Décimation directe. — Les lettres d'un alphabet étant disposées en cercle, comptons, à partir d'une lettre convenue, de un à dix et prélevons la dixième lettre ; recommençons à compter jus-

qu'à dix et prélevons la vingtième; en continuant de la sorte, sans tenir compte des lettres déjà enlevées, nous formerons un alphabet complet et absolument interverti.

Supposons qu'on ait pris l'alphabet normal de vingt-cinq lettres et qu'on commence le décompte à A; on dira 1 sur A, 2 sur B, ... 10 sur J; ayant prélevé J, on recommencera 1 sur K, 2 sur L, ... 10 sur T; on met T à la suite de J. On trouve de même 10 sur E, puis 10 sur P, la lettre J ne comptant plus.....

On obtient finalement l'alphabet interverti suivant :

JTEPBNAODSIZUMKHLRYQGXCVF.

L'alphabet normal de vingt-six lettres aurait donné :

JTDOZLXKYNCSIEWURVBHAQGMFP.

Décimation inverse. — Ayant préparé un nombre de cases égal à celui des lettres de l'alphabet, on pose la première lettre A dans la dixième case, B dans la vingtième, C dans la 5ᵉ = 30 — 25 (ou dans la 4ᵉ = 30 — 26), et, en ne comptant que les cases vides.

On obient ainsi, avec l'alphabet normal

de vingt-cinq lettres : GEXICZUPKAOQNFHDTRJBMYVSL ;
de vingt-six lettres : USKCNYWTMAHFXJDZVQLBPROGIE.

Le point de départ de la décimation est arbitraire, ainsi que le nombre par lequel on décime, car dix peut être remplacé par tout autre nombre et même par plusieurs revenant périodiquement.

On peut également, au lieu de l'alphabet normal, décimer un alphabet interverti ou déjà décimé et on a ainsi une décimation double, triple, etc.

Nous ne croyons pas utile de nous étendre davantage sur la décimation bien que ce genre de calcul donne lieu à de curieux problèmes d'*analyse combinatoire*.

Notons cependant que la décimation peut être grandement facilitée par l'emploi de cartons portant chacun une lettre alphabétique et pouvant être maniés aussi facilement qu'un jeu de cartes.

Systèmes polyalphabétiques. — Reprenons les *bandes alphabétiques* décrites à la page 30 et remplaçons l'alphabet normal par un alphabet interverti, KLAGENFURTH ...., par exemple. Formons un tableau semblable à celui que nous avons construit avec l'alphabet normal et nous aurons :

n	i	d	l	z	a	f	b	m	e	l
f	j	i	a	k	g	u	c	o	n	a
u	m	j	g	l	e	r	d	p	f	g
R	O	M	E	A	N	T	I	Q	U	E
t	p	o	n	g	f	h	j	s	r	n
h	q	p	f	e	u	b	m	v	t	f
b	s	q	u	n	r	c	o	w	h	u
c	v	s	r	f	t	d	p	x	b	r
d	w	v	t	u	h	i	q	y	c	t

Si la clé est simple, c'est-à-dire la même pour toutes les lettres du clair, notre texte sera cryptographié par une ligne quelconque du tableau, par exemple par celle qui suit le texte ; on aura donc :

ROME ANTIQUE = *tpongfhjsrn*.

Mais si, à l'aide du chiffre carré formé avec le même alphabet, page 37, nous cherchons la clé de ce cryptogramme, nous sommes conduits à constater que cette clé n'existe pas, car elle change à chaque lettre ; dans le cas présent, on trouve : *sefbdtrheob*.

Il en serait de même avec l'*obturateur en escalier*, comme le prouve le diagramme :

u	m	j	g	l	e	r	d	p	f	g	
R	O	M	E	A	N	T	I	Q	U	E	
»	»	»	»	»	»	»	»	»	»	»	»
»	»	p	»	»	u	»	»	v	»	»	
b	»	q	u	»	r	c	»	w	h	»	
c	v	s	r	f	t	d	p	x	b	r	
d	w	v	t	u	h	i	q	y	c	t	

qui nous fournira : ROME ANTIQUE = *bvpufucpvhr*, dont la clé semble être : *uhgdgutkfqe*.

Ces résultats prouvent évidemment que le chiffre carré auquel nous nous référons n'est pas celui qui a servi au chiffrement. Pour trouver ce dernier, opérons comme nous avons fait pour obtenir le tableau de Vigenère, c'est-à-dire, faisons glisser nos bandes alphabétiques de manière à amener, à la première ligne horizontale, toutes les lettres de l'alphabet *dans leur ordre normal,* ce qui formera le tableau suivant, que nous jugeons inutile de reproduire en entier :

Clés																			
A-K	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	...
B-L	G	C	D	I	N	U	E	B	J	M	L	A	O	F	P	Q	S	T	.
C-A	E	D	I	J	F	R	N	C	M	O	A	G	P	U	Q	S	V	H	
D-G	N	I	J	M	U	T	F	D	O	P	G	E	Q	R	S	V	W		
E-E	F	J	M	O	R	H	U	I	P	Q	E	N	S	T	V				
F-N	U	M	O	P	T	B	R	J	Q	S	N	F	V	H					
G-F	R	O	P	Q	H	C	T	M	S	V	F	U							
H-U	T	P	Q	S	B	D	H	O	V										
I-R	H	Q	S	V	C	I	B												
J-T	B	S	V	W	D														
K-H	C	V	W																
L-B	D	W																	

En cryptographiant : ROME ANTIQUE, à l'aide de ce tableau, la clé B donne *tpongfhjsrn* et la clé DEC : *bvpufucpvhr*, c'est-à-dire les mêmes cryptogrammes que les bandes alphabétiques.

Si, au lieu de prendre les lettres-clés dans l'alphabet normal, nous les avions lues dans l'alphabet interverti, nous aurions L à la place de B et GEA à la place de DEC.

Ce nouveau chiffre carré ne diffère de celui de la page 37 que par l'interversion des colonnes, interversion nécessitée par le classement dans leur ordre normal des lettres du premier sous-alphabet. Cette simple modification a suffi pour apporter de sérieux avantages au dernier tableau, dont la formation n'offre d'ailleurs pas plus de difficultés.

Ces avantages sont :

1° La suppression de la symétrie horizontale, d'où résulte la formation de nouveaux alphabets intervertis *tous différents les uns des autres*, qui prennent le nom d'*alphabets secondaires*.

2° La facilité de traduction par l'emploi de *sous-clés* ou *clés complémentaires*, ce qui évite la recherche des lettres dans les

alphabets intervertis et permet de traduire aussi facilement que l'on chiffre.

Voici le tableau des sous-clés pour chacun des alphabets :

Alph. normal....	A	B	C	D	E	F	G	H	I	J	K	L	M	N
	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N
Alph. interverti..	K	L	A	G	E	N	F	U	R	T	H	B	C	D
	K	Z	Y	X	W	V	S	Q	P	O	M	J	I	D

Le mode d'emploi est simple : Supposons qu'on ait à traduire une dépêche chiffrée avec la clé G prise dans l'alphabet normal (ou F dans l'alphabet interverti), il suffira, pour *traduire*, de *chiffrer le cryptogramme* avec la clé U (alphabet normal) ou S (alphabet interverti), pour trouver le texte clair :

b v p u
x w y x ... complément de DEC et de GEA.
R O M E

Bandes polyalphabétiques. — Jusqu'ici, les bandes que nous avons considérées portent toutes le même alphabet, ce qui n'est qu'un cas particulier de la méthode générale, consistant à inscrire, sur chaque bande, un alphabet différent.

On se sert de ces bandes comme de celles dont nous nous sommes déjà occupé.

Exemple :

z	s	x	g	y	l	z	o	s	j	r
a	p	z	l	e	s	g	n	t	a	i
L	A	C	A	V	A	L	E	R	I	E
o	v	h	f	i	i	o	u	u	m	l
n	d	a	n	t	c	i	r	e	e	s
s	t	r	c	z	u	r	t	z	l	o
e	o	y	b	l	x	e	p	l	o	n
f	y	b	h	s	b	m	a	a	g	a

Nous prendrons pour cryptogramme du texte clair :

LA CAVALERIE

la ligne dont le numéro est fixé par les conventions, ou même, si le nombre des bandes employées est assez grand pour que le

clair puisse être reconnu sans aucune ambiguïté, nous prendrons une ligne quelconque.

Pour faciliter les combinaisons et augmenter les garanties de secret, on donne un numéro à chaque bande ; il est, en outre, utile de les faire commencer par des lettres différentes. La convention peut ainsi fixer par un mot-clé l'ordre dans lequel les bandes doivent être disposées.

Ce système sert de base à diverses méthodes et même à des appareils très ingénieux, tel que celui inventé par M. le capitaine Bazeries.

A la clé simple ou monolittérale, nous pouvons, à l'aide de *l'obturateur en escalier*, simple ou double, substituer une clé polylittérale, dont nous avons déjà vu l'emploi.

Cet obturateur a donné naissance aux *grilles chiffrantes*, que nous étudierons après avoir reconnu la richesse des combinaisons que peuvent former deux bandes alphabétiques simplement juxtaposées.

—	0
—	1
—	2
—	3
—	—
—	—
24	—
25	—
0	D
1	—
2	—
—	—
—	—
—	—
E	F
—	—

Formules cryptographiques. — Prenons deux bandes ou réglettes portant à intervalles égaux, au lieu des lettres de l'alphabet, les nombres de 0 à 25 ; juxtaposons ces deux réglettes et nous constaterons aisément que, dans toutes les positions possibles, les nombres des deux réglettes situés au même niveau ont une différence constante, égale au nombre qui, dans l'une, correspond au zéro de l'autre ; deux lignes quelconques de ces bandes fournissent donc quatre quantités en proportion arithmétique.

Les quatre quantités : 0, D, E, F, donnent le diagramme :

$$\begin{array}{c|c} 0 & D \\ E & F \end{array}$$

Représentant par l la lettre à cryptographier, par c la base du chiffrement, c'est-à-dire, la clé, et par x le chiffre de l, et faisant :

	N° 1	N° 1 bis	N° 2	N° 2 bis	N° 3	N° 3 bis
	$D = c$	$D = l$	$D = x$	$D = l$	$D = c$	$D = x$
	$E = l$	$E = c$	$E = l$	$E = x$	$E = x$	$E = c$
	$F = x$	$F = x$	$F = c$	$F = c$	$F = l$	$F = l$
On aura :	$\begin{array}{c\|c} 0 & c \\ l & x \end{array}$	$\begin{array}{c\|c} 0 & l \\ c & x \end{array}$	$\begin{array}{c\|c} 0 & x \\ l & c \end{array}$	$\begin{array}{c\|c} 0 & l \\ x & c \end{array}$	$\begin{array}{c\|c} 0 & c \\ x & l \end{array}$	$\begin{array}{c\|c} 0 & x \\ c & l \end{array}$
Soit :	$x = c + l$		$x = c - l$		$x = l - c$	

Nous ne tiendrons aucun compte des diagrammes 1 *bis*, 2 *bis*, 3 et 3 *bis*, qui donnent les mêmes résultats que les premiers en changeant parfois l'alphabet dans lequel est lue la clé, c'est-à-dire en transformant l'apparence de celle-ci, *sans changer sa valeur numérique* (voir page 50).

En remplaçant les séries numériques des réglettes par l'alphabet normal : A = 0, B = 1, C = 2..... Z = 25, et en donnant successivement à la clé toutes les valeurs de 0 à 25, nous aurons le chiffre carré de Vigenère, avec la première formule, tandis que la deuxième fournira le chiffre carré de Beaufort.

Si, à la série numérique de l'une ou des deux bandes, on substitue un alphabet interverti, tel par exemple que : K = 0, L = 1, A = 2, G = 3..... Z = 25, on obtiendra, avec la première équation, un chiffre carré interverti, type Vigenère, comme celui de la page 50; la deuxième équation donne un chiffre carré interverti du type Beaufort.

Dans la moitié des cas, les chiffres carrés obtenus présentent l'inconvénient de la *symétrie horizontale* et ne fournissant que des *sous-alphabets*, c'est-à-dire l'alphabet *primaire* débutant successivement par chaque lettre, mais conservant sa séquence propre.

Il n'en est pas de même quand on se sert, pour la première bande, d'un alphabet interverti, l'autre bande pouvant porter un alphabet quelconque interverti ou non.

Dans ce cas, l'ordre des colonnes est interverti et la différence entre les valeurs de deux lettres se suivant dans l'alphabet normal n'est plus égal à l'unité; elle est variable, selon l'alphabet adopté, mais constante dans toute l'étendue des colonnes appartenant à ces deux lettres.

De ce qui précède, il résulte que, par le simple rapprochement de deux bandes ou réglettes portant chacune un alphabet, on peut obtenir tous les alphabets constituant deux séries de chiffres carrés; l'une du type de Vigenère, et la seconde du chiffre de Beaufort.

La position des *éléments du chiffrage* est indiquée dans les diagrammes ci-après où, comme précédemment, 0 représente l'origine ou la première lettre de chaque alphabet, c la clé, *l* la lettre à cryptographier et *x* son chiffre :

Système Vigenère

A	B
0	c
l	*x*

Système Beaufort

A	B
0	*x*
l	c

ce qui correspond aux équations : $x^B = c^B + l^A$ et $x^B = c^B - l^A$.

Les exposants indiquent l'alphabet dans lequel chaque lettre doit être lue.

En changeant les réglettes de place, on obtient les deux nouvelles équations : $x^A = c^A + l^B$ et $x^A = c^A - l^B$; et, en employant deux bandes identiques, on a :

avec A. . . . . . $x^A = c^A + l^A$ et $x^A = c^A - l^A$

et avec B. . . . . $x^B = c^B + l^B$ et $x^B = c^B - l^B$

En résumé, deux alphabets inscrits sur quatre bandes (identiques deux à deux) ont la valeur de *huit* chiffres carrés et mettent à notre disposition $8 \times 26 = 208$ alphabets ou sous-alphabets différents.

Les tableaux qui suivent présentent les *huit chiffres carrés* obtenus avec deux bandes portant l'une, A, l'alphabet normal, et l'autre, B, l'alphabet :

F L R X D K S Z H P Y I T C O B Q G W U N V E A M J

fourni par la décimation directe, par six, de l'alphabet de vingt-six lettres, au départ de F.

Pour cryptographier avec ces tableaux, on opère comme avec celui de Vigenère, en lisant la lettre à chiffrer dans l'alphabet horizontal, la clé dans l'alphabet vertical et le chiffre à l'intersection de la colonne de la première et de la rangée de la seconde.

FORMULE

A	A
0	c
l	x

$x^{A} = c^{A} + l^{A}$

Tableau N° 1

Symétries horizontale et verticale.

SYSTÈME DE VIGENÈRE

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

FORMULE

A	B
0	c
l	x

Tableau N° 2

Symétrie horizontale.

SYSTÈME DE VIGENÈRE

$$x^B = c^B + l^A$$

Clés A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	M	J	F	L	R	X	D	K	S	Z	H	P	Y	I	T	C	O	B	Q	G	W	U	N	V	E
B	Q	G	W	U	N	V	E	A	M	J	F	L	R	X	D	K	S	Z	H	P	Y	I	T	C	O
C	O	B	Q	G	W	U	N	V	E	A	M	J	F	L	R	X	D	K	S	Z	H	P	Y	I	T
D	K	S	Z	H	P	Y	I	T	C	O	B	Q	G	W	U	N	V	E	A	M	J	F	L	R	X
E	A	M	J	F	L	R	X	D	K	S	Z	H	P	Y	I	T	C	O	B	Q	G	W	U	N	V
F	L	R	X	D	K	S	Z	H	P	Y	I	T	C	O	B	Q	G	W	U	N	V	E	A	M	J
G	W	U	N	V	E	A	M	J	F	L	R	X	D	K	S	Z	H	P	Y	I	T	C	O	B	Q
H	P	Y	I	T	C	O	B	Q	G	W	U	N	V	E	A	M	J	F	L	R	X	D	K	S	Z
I	T	C	O	B	Q	G	W	U	N	V	E	A	M	J	F	L	R	X	D	K	S	Z	H	P	Y
J	F	L	R	X	D	K	S	Z	H	P	Y	I	T	C	O	B	Q	G	W	U	N	V	E	A	M
K	S	Z	H	P	Y	I	T	C	O	B	Q	G	W	U	N	V	E	A	M	J	F	L	R	X	D
L	R	X	D	K	S	Z	H	P	Y	I	T	C	O	B	Q	G	W	U	N	V	E	A	M	J	F
M	J	F	L	R	X	D	K	S	Z	H	P	Y	I	T	C	O	B	Q	G	W	U	N	V	E	A
N	V	E	A	M	J	F	L	R	X	D	K	S	Z	H	P	Y	I	T	C	O	B	Q	G	W	U
O	B	Q	G	W	U	N	V	E	A	M	J	F	L	R	X	D	K	S	Z	H	P	Y	I	T	C
P	Y	I	T	C	O	B	Q	G	W	U	N	V	E	A	M	J	F	L	R	X	D	K	S	Z	H
Q	G	W	U	N	V	E	A	M	J	F	L	R	X	D	K	S	Z	H	P	Y	I	T	C	O	B
R	X	D	K	S	Z	H	P	Y	I	T	C	O	B	Q	G	W	U	N	V	E	A	M	J	F	L
S	Z	H	P	Y	I	T	C	O	B	Q	G	W	U	N	V	E	A	M	J	F	L	R	X	D	K
T	C	O	B	Q	G	W	U	N	V	E	A	M	J	F	L	R	X	D	K	S	Z	H	P	Y	I
U	N	V	E	A	M	J	F	L	R	X	D	K	S	Z	H	P	Y	I	T	C	O	B	Q	G	W
V	E	A	M	J	F	L	R	X	D	K	S	Z	H	P	Y	I	T	C	O	B	Q	G	W	U	N
W	U	N	V	E	A	M	J	F	L	R	X	D	K	S	Z	H	P	Y	I	T	C	O	B	Q	G
X	D	K	S	Z	H	P	Y	I	T	C	O	B	Q	G	W	U	N	V	E	A	M	J	F	L	R
Y	I	T	C	O	B	Q	G	W	U	N	V	E	A	M	J	F	L	R	X	D	K	S	Z	H	P
Z	H	P	Y	I	T	C	O	B	Q	G	W	U	N	V	E	A	M	J	F	L	R	X	D	K	S

FORMULE

B	A
0	c
l	x

Tableau N° 3

Symétrie verticale.

SYSTÈME DE VIGENÈRE

$$x^{A} = c^{A} + l^{B}$$

Clés	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	X	P	N	E	W	A	R	I	L	Z	F	B	Y	U	O	J	Q	C	G	M	T	V	S	D	K	H
B	Y	Q	O	F	X	B	S	J	M	A	G	C	Z	V	P	K	R	D	H	N	U	W	T	E	L	I
C	Z	R	P	G	Y	C	T	K	N	B	H	D	A	W	Q	L	S	E	I	O	V	X	U	F	M	J
D	A	S	Q	H	Z	D	U	L	O	C	I	E	B	X	R	M	T	F	J	P	W	Y	V	G	N	K
E	B	T	R	I	A	E	V	M	P	D	J	F	C	Y	S	N	U	G	K	Q	X	Z	W	H	O	L
F	C	U	S	J	B	F	W	N	Q	E	K	G	D	Z	T	O	V	H	L	R	Y	A	X	I	P	M
G	D	V	T	K	C	G	X	O	R	F	L	H	E	A	U	P	W	I	M	S	Z	B	Y	J	Q	N
H	E	W	U	L	D	H	Y	P	S	G	M	I	F	B	V	Q	X	J	N	T	A	C	Z	K	R	O
I	F	X	V	M	E	I	Z	Q	T	H	N	J	G	C	W	R	Y	K	O	U	B	D	A	L	S	P
J	G	Y	W	N	F	J	A	R	U	I	O	K	H	D	X	S	Z	L	P	V	C	E	B	M	T	Q
K	H	Z	X	O	G	K	B	S	V	J	P	L	I	E	Y	T	A	M	Q	W	D	F	C	N	U	R
L	I	A	Y	P	H	L	C	T	W	K	Q	M	J	F	Z	U	B	N	R	X	E	G	D	O	V	S
M	J	B	Z	Q	I	M	D	U	X	L	R	N	K	G	A	V	C	O	S	Y	F	H	E	P	W	T
N	K	C	A	R	J	N	E	V	Y	M	S	O	L	H	B	W	D	P	T	Z	G	I	F	Q	X	U
O	L	D	B	S	K	O	F	W	Z	N	T	P	M	I	C	X	E	Q	U	A	H	J	G	R	Y	V
P	M	E	C	T	L	P	G	X	A	O	U	Q	N	J	D	Y	F	R	V	B	I	K	H	S	Z	W
Q	N	F	D	U	M	Q	H	Y	B	P	V	R	O	K	E	Z	G	S	W	C	J	L	I	T	A	X
R	O	G	E	V	N	R	I	Z	C	Q	W	S	P	L	F	A	H	T	X	D	K	M	J	U	B	Y
S	P	H	F	W	O	S	J	A	D	R	X	T	Q	M	G	B	I	U	Y	E	L	N	K	V	C	Z
T	Q	I	G	X	P	T	K	B	E	S	Y	U	R	N	H	C	J	V	Z	F	M	O	L	W	D	A
U	R	J	H	Y	Q	U	L	C	F	T	Z	V	S	O	I	D	K	W	A	G	N	P	M	X	E	B
V	S	K	I	Z	R	V	M	D	G	U	A	W	T	P	J	E	L	X	B	H	O	Q	N	Y	F	C
W	T	L	J	A	S	W	N	E	H	V	B	X	U	Q	K	F	M	Y	C	I	P	R	O	Z	G	D
X	U	M	K	B	T	X	O	F	I	W	C	Y	V	R	L	G	N	Z	D	J	Q	S	P	A	H	E
Y	V	N	L	C	U	Y	P	G	J	X	D	Z	W	S	M	H	O	A	E	K	R	T	Q	B	I	F
Z	W	O	M	D	V	Z	Q	H	K	Y	E	A	X	T	N	I	P	B	F	L	S	U	R	C	J	G

FORMULE

B	B
0	c
l	x

TABLEAU N° 4

Pas de symétrie.

SYSTÈME DE VIGENÈRE

$$x^B = c^B + l^B$$

Clés	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	N	T	Y	L	U	A	O	K	H	E	R	M	V	G	I	S	C	J	X	P	Q	W	B	F	Z	D
B	T	D	R	U	I	B	S	A	F	O	N	Q	C	P	X	M	K	G	V	L	H	Y	Z	W	J	E
C	Y	R	F	G	P	C	D	V	M	T	W	O	I	Z	L	E	X	B	U	J	S	H	K	Q	A	N
D	L	U	G	H	F	D	V	T	B	X	P	K	R	M	W	C	N	S	Y	Q	A	J	E	Z	O	I
E	U	I	P	F	W	E	C	D	Z	V	L	A	N	Q	Y	K	T	M	R	H	B	G	O	J	S	X
F	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
G	O	S	D	V	C	G	H	J	R	Q	E	W	B	I	K	F	Z	U	A	X	Y	T	P	N	L	M
H	K	A	V	T	D	H	J	Q	U	Z	C	P	S	R	E	G	M	Y	O	N	L	X	F	I	W	B
I	H	F	M	B	Z	I	R	U	E	Y	Q	T	P	K	J	N	L	C	G	A	D	S	X	O	V	W
J	E	O	T	X	V	J	Q	Z	Y	M	D	F	A	U	C	H	B	L	K	I	W	N	G	R	P	S
K	R	N	W	P	L	K	E	C	Q	D	Y	S	X	J	U	O	V	Z	I	G	M	F	A	H	B	T
L	M	Q	O	K	A	L	W	P	T	F	S	R	J	V	B	Y	G	X	Z	C	N	E	U	D	I	H
M	V	C	I	R	N	M	B	S	P	A	X	J	E	W	T	Z	O	F	D	Y	G	U	Q	L	H	K
N	G	P	Z	M	Q	N	I	R	K	U	J	V	W	O	H	X	Y	E	F	S	C	B	T	A	D	L
O	I	X	L	W	Y	O	K	E	J	C	U	B	T	H	R	A	D	Q	N	F	Z	P	S	G	M	V
P	S	M	E	C	K	P	F	G	N	H	O	Y	Z	X	A	W	J	I	B	V	R	D	L	T	U	Q
Q	C	K	X	N	T	Q	Z	M	L	B	V	G	O	Y	D	J	S	W	E	R	P	I	H	U	F	A
R	J	G	B	S	M	R	U	Y	C	L	Z	X	F	E	Q	I	W	D	H	O	V	A	N	K	T	P
S	X	V	U	Y	R	S	A	O	G	K	I	Z	D	F	N	B	E	H	T	W	J	L	M	P	Q	C
T	P	L	J	Q	H	T	X	N	A	I	G	C	Y	S	F	V	R	O	W	M	K	Z	D	B	E	U
U	Q	H	S	A	B	U	Y	L	D	W	M	N	G	C	Z	R	P	V	J	K	T	O	I	E	X	F
V	W	Y	H	J	G	V	T	X	S	N	F	E	U	B	P	D	I	A	L	Z	O	Q	C	M	K	R
W	B	Z	K	E	O	W	P	F	X	G	A	U	Q	T	S	L	H	N	M	D	I	C	Y	V	R	J
X	F	W	Q	Z	J	X	N	I	O	R	H	D	L	A	G	T	U	K	P	B	E	M	V	S	C	Y
Y	Z	J	A	O	S	Y	L	W	V	P	B	I	H	D	M	U	F	T	Q	E	X	K	R	C	N	G
Z	D	E	N	I	X	Z	M	B	W	S	T	H	K	L	V	Q	A	P	C	U	F	R	J	Y	G	O

Symétries horizontale et verticale.

Lettres couplées.

TABLEAU Nº 5

SYSTÈME DE BEAUFORT

FORMULE

$$\left| \begin{array}{c|c} A & A \\ \hline 0 & x \\ l & c \end{array} \right|$$

$$x^{A} = c^{A} - l^{A}$$

Clés A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B
B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C
C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D
D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E
E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F
F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G
G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H
H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I
I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J
J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K
K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L
L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M
M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N
N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O
O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P
P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q
Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R
R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S
S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T
T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U
U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V
V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W
W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X
X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y
Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z
Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A

FORMULE

A	B
0	x
l	c

Tableau N° 6

Symétrie horizontale.

SYSTÈME DE BEAUFORT

$$x^{B} = c^{B} - l^{A}$$

Clés A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	E	V	N	U	W	G	Q	B	O	C	T	I	Y	P	H	Z	S	K	D	X	R	L	F	J	M
B	O	C	T	I	Y	P	H	Z	S	K	D	X	R	L	F	J	M	A	E	V	N	U	W	G	Q
C	T	I	Y	P	H	Z	S	K	D	X	R	L	F	J	M	A	E	V	N	U	W	G	Q	B	O
D	X	R	L	F	J	M	A	E	V	N	U	W	G	Q	B	O	C	T	I	Y	P	H	Z	S	K
E	V	N	U	W	G	Q	B	O	C	T	I	Y	P	H	Z	S	K	D	X	R	L	F	J	M	A
F	J	M	A	E	V	N	U	W	G	Q	B	O	C	T	I	Y	P	H	Z	S	K	D	X	R	L
G	Q	B	O	C	T	I	Y	P	H	Z	S	K	D	X	R	L	F	J	M	A	E	V	N	U	W
H	Z	S	K	D	X	R	L	F	J	M	A	E	V	N	U	W	G	Q	B	O	C	T	I	Y	P
I	Y	P	H	Z	S	K	D	X	R	L	F	J	M	A	E	V	N	U	W	G	Q	B	O	C	T
J	M	A	E	V	N	U	W	G	Q	B	O	C	T	I	Y	P	H	Z	S	K	D	X	R	L	F
K	D	X	R	L	F	J	M	A	E	V	N	U	W	G	Q	B	O	C	T	I	Y	P	H	Z	S
L	F	J	M	A	E	V	N	U	W	G	Q	B	O	C	T	I	Y	P	H	Z	S	K	D	X	R
M	A	E	V	N	U	W	G	Q	B	O	C	T	I	Y	P	H	Z	S	K	D	X	R	L	F	J
N	U	W	G	Q	B	O	C	T	I	Y	P	H	Z	S	K	D	X	R	L	F	J	M	A	E	V
O	C	T	I	Y	P	H	Z	S	K	D	X	R	L	F	J	M	A	E	V	N	U	W	G	Q	B
P	H	Z	S	K	D	X	R	L	F	J	M	A	E	V	N	U	W	G	Q	B	O	C	T	I	Y
Q	B	O	C	T	I	Y	P	H	Z	S	K	D	X	R	L	F	J	M	A	E	V	N	U	W	G
R	L	F	J	M	A	E	V	N	U	W	G	Q	B	O	C	T	I	Y	P	H	Z	S	K	D	X
S	K	D	X	R	L	F	J	M	A	E	V	N	U	W	G	Q	B	O	C	T	I	Y	P	H	Z
T	I	Y	P	H	Z	S	K	D	X	R	L	F	J	M	A	E	V	N	U	W	G	Q	B	O	C
U	W	G	Q	B	O	C	T	I	Y	P	H	Z	S	K	D	X	R	L	F	J	M	A	E	V	N
V	N	U	W	G	Q	B	O	C	T	I	Y	P	H	Z	S	K	D	X	R	L	F	J	M	A	E
W	G	Q	B	O	C	T	I	Y	P	H	Z	S	K	D	X	R	L	F	J	M	A	E	V	N	U
X	R	L	F	J	M	A	E	V	N	U	W	G	Q	B	O	C	T	I	Y	P	H	Z	S	K	D
Y	P	H	Z	S	K	D	X	R	L	F	J	M	A	E	V	N	U	W	G	Q	B	O	C	T	I
Z	S	K	D	X	R	L	F	J	M	A	E	V	N	U	W	G	Q	B	O	C	T	I	Y	P	H

FORMULE

B	A
0	c
l	x

TABLEAU N° 7

Symétrie verticale.

SYSTÈME DE BEAUFORT

$$x^{A} = c^{A} - l^{B}$$

Clés	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	D	L	N	W	E	A	J	S	P	B	V	Z	C	G	M	R	K	Y	U	O	H	F	I	X	Q	T
B	E	M	O	X	F	B	K	T	Q	C	W	A	D	H	N	S	L	Z	V	P	I	G	J	Y	R	U
C	F	N	P	Y	G	C	L	U	R	D	X	B	E	I	O	T	M	A	W	Q	J	H	K	Z	S	V
D	G	O	Q	Z	H	D	M	V	S	E	Y	C	F	J	P	U	N	B	X	R	K	I	L	A	T	W
E	H	P	R	A	I	E	N	W	T	F	Z	D	G	K	Q	V	O	C	Y	S	L	J	M	B	U	X
F	I	Q	S	B	J	F	O	X	U	G	A	E	H	L	R	W	P	D	Z	T	M	K	N	C	V	Y
G	J	R	T	C	K	G	P	Y	V	H	B	F	I	M	S	X	Q	E	A	U	N	L	O	D	W	Z
H	K	S	U	D	L	H	Q	Z	W	I	C	G	J	N	T	Y	R	F	B	V	O	M	P	E	X	A
I	L	T	V	E	M	I	R	A	X	J	D	H	K	O	U	Z	S	G	C	W	P	N	Q	F	Y	B
J	M	U	W	F	N	J	S	B	Y	K	E	I	L	P	V	A	T	H	D	X	Q	O	R	G	Z	C
K	N	V	X	G	O	K	T	C	Z	L	F	J	M	Q	W	B	U	I	E	Y	R	P	S	H	A	D
L	O	W	Y	H	P	L	U	D	A	M	G	K	N	R	X	C	V	J	F	Z	S	Q	T	I	B	E
M	P	X	Z	I	Q	M	V	E	B	N	H	L	O	S	Y	D	W	K	G	A	T	R	U	J	C	F
N	Q	Y	A	J	R	N	W	F	C	O	I	M	P	T	Z	E	X	L	H	B	U	S	V	K	D	G
O	R	Z	B	K	S	O	X	G	D	P	J	N	Q	U	A	F	Y	M	I	C	V	T	W	L	E	H
P	S	A	C	L	T	P	Y	H	E	Q	K	O	R	V	B	G	Z	N	J	D	W	U	X	M	F	I
Q	T	B	D	M	U	Q	Z	I	F	R	L	P	S	W	C	H	A	O	K	E	X	V	Y	N	G	J
R	U	C	E	N	V	R	A	J	G	S	M	Q	T	X	D	I	B	P	L	F	Y	W	Z	O	H	K
S	V	D	F	O	W	S	B	K	H	T	N	R	U	Y	E	J	C	Q	M	G	Z	X	A	P	I	L
T	W	E	G	P	X	T	C	L	I	U	O	S	V	Z	F	K	D	R	N	H	A	Y	B	Q	J	M
U	X	F	H	Q	Y	U	D	M	J	V	P	T	W	A	G	L	E	S	O	I	B	Z	C	R	K	N
V	Y	G	I	R	Z	V	E	N	K	W	Q	U	X	B	H	M	F	T	P	J	C	A	D	S	L	O
W	Z	H	J	S	A	W	F	O	L	X	R	V	Y	C	I	N	G	U	Q	K	D	B	E	T	M	P
X	A	I	K	T	B	X	G	P	M	Y	S	W	Z	D	J	O	H	V	R	L	E	C	F	U	N	Q
Y	B	J	L	U	C	Y	H	Q	N	Z	T	X	A	E	K	P	I	W	S	M	F	D	G	V	O	R
Z	C	K	M	V	D	Z	I	R	O	A	U	Y	B	F	L	Q	J	X	T	N	G	E	H	W	P	S

Pas de symétrie.

Lettres couplées.

TABLEAU N° 8

FORMULE

$$\left|\begin{array}{c|c} B & B \\ \hline 0 & x \\ l & c \end{array}\right|$$

SYSTÈME DE BEAUFORT

$$x^{B} = c^{B} - l^{B}$$

Clés	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	F	H	Y	U	L	A	S	B	T	M	W	E	J	X	P	O	Z	V	G	I	D	R	K	N	C	Q
B	W	F	R	I	U	B	M	Z	D	Q	Y	O	G	V	L	S	J	C	P	X	E	N	A	T	K	H
C	Q	M	F	P	G	C	E	K	R	O	H	T	B	U	J	D	A	I	Z	L	N	W	V	Y	X	S
D	Z	B	G	F	H	D	C	E	U	K	J	X	S	Y	Q	V	O	R	M	W	I	P	T	L	N	A
E	J	Z	P	W	F	E	K	O	I	A	G	V	M	R	H	C	S	N	Q	Y	X	L	D	U	T	B
F	X	I	C	E	D	F	P	W	B	L	V	J	R	S	T	G	Y	M	N	O	Z	K	H	A	Q	U
G	N	R	D	C	V	G	F	P	S	W	T	Q	U	A	X	H	L	B	I	K	M	E	J	O	Z	Y
H	I	U	V	D	T	H	G	F	A	P	X	Z	Y	O	N	J	W	S	R	E	B	C	Q	K	M	L
I	O	E	M	Z	B	I	N	X	F	T	S	Y	C	G	A	R	V	P	K	J	W	Q	U	H	L	D
J	R	Y	T	V	X	J	H	G	O	F	N	M	L	K	I	Q	P	A	U	C	S	D	Z	E	B	W
K	H	Q	W	L	P	K	O	A	N	S	F	D	Z	I	G	E	B	X	J	U	T	Y	C	R	V	M
L	D	T	O	A	K	L	Y	U	Q	R	E	F	X	Z	C	W	I	J	V	B	H	S	P	M	G	N
M	L	P	I	N	R	M	Z	Q	C	J	U	A	F	D	Y	B	H	E	W	T	K	X	S	V	O	G
N	A	K	Z	Q	M	N	X	T	P	V	B	U	E	F	S	I	D	W	O	H	L	J	R	G	Y	C
O	G	J	L	Y	W	O	A	S	X	B	P	C	Q	N	F	K	M	T	H	R	V	U	E	I	D	Z
P	T	N	E	K	C	P	W	L	M	Y	D	H	I	B	V	F	U	Z	X	A	Q	O	G	S	J	R
Q	U	L	X	T	N	Q	J	H	K	G	I	B	W	E	R	Z	F	O	Y	D	A	V	M	C	S	P
R	K	C	B	M	S	R	I	N	G	X	A	L	D	H	O	U	T	F	E	Q	P	Z	Y	J	W	V
S	P	G	U	R	Y	S	B	M	V	Z	L	K	H	T	W	A	Q	D	F	N	C	I	O	X	E	J
T	B	A	J	H	Q	T	V	D	L	C	Z	I	O	W	M	X	E	Y	S	F	U	G	N	P	R	K
U	E	D	S	B	A	U	R	I	H	N	O	W	V	J	K	Y	X	G	C	Z	F	M	L	Q	P	T
V	M	S	H	G	J	V	D	C	Y	E	Q	N	A	L	Z	T	K	U	B	P	R	F	X	W	I	O
W	V	X	K	O	E	W	L	Y	Z	U	C	G	N	M	D	P	R	Q	T	S	J	A	F	B	H	I
X	S	O	Q	J	Z	X	T	V	W	D	M	R	K	P	B	N	C	L	A	G	Y	H	I	F	U	E
Y	C	V	A	S	O	Y	U	R	J	I	K	P	T	Q	E	L	N	H	D	M	G	B	W	Z	F	X
Z	Y	W	N	X	I	Z	Q	J	E	H	R	S	P	C	U	M	G	K	L	V	O	T	B	D	A	F

Il importe de rappeler que la *symétrie de position* ou *symétrie horizontale a pour unique cause la lecture de la lettre à chiffrer dans l'alphabet normal* (1).

En supprimant les quatre formules qui présentent cette particularité, les quatre autres fournissent $4 \times 26 = 104$ *alphabets différents*.

Les bandes alphabétiques permettent la suppression complète des chiffres carrés et simplifient étonnamment tous les systèmes dérivés du tableau de Vigenère.

Pour bien faire ressortir l'exactitude de cette assertion, nous ferons l'application de nos formules à la méthode imaginée par M. le capitaine de Calbiac.

Méthode de M. le capitaine de Calbiac. — Cette originale et curieuse méthode, qui est un mélange des systèmes de Vigenère et de Beaufort, additionné d'autochiffrement et de transposition, exige, d'après son auteur, la formation d'un alphabet numérique interverti et l'emploi d'un carré de six cent soixante-seize cases dont chacune renferme deux lettres et dont, par suite, la confection est longue et laborieuse ; délicates et pénibles sont aussi les recherches à faire dans ce tableau.

On obtient les mêmes cryptogrammes à l'aide de deux bandes alphabétiques, dont un seul mouvement fournit les deux chiffres de chaque groupe.

En effet si, pour abréger l'écriture, nous représentons

par *a.b* *c.d* *e.f* *g.h* ..... les lettres claires
et par A.B C.D E.F G.H .... les chiffres

à inscrire sous chaque lettre, nous pourrons, en supposant déjà déterminé $B = a - b$, trouver dans la même position des bandes, les deux chiffres C et D du deuxième groupe ; de même D nous donnera les chiffres E et F du troisième groupe ; F fournira les chiffres G et H du quatrième groupe, etc., comme le montrent les diagrammes ci-dessous, où o représente la première lettre de l'alphabet A :

(A)	(B)		(A)	(B)		(A)	(B)
—	—		—	—		—	—
o	*d*		o	*f*		o	*h*
B	C		D	E		F	G
D	*c*		F	*e*		H	*g*

La traduction est donnée par les mêmes positions des bandes, *c.d*, *e.f*, *g.h* .... étant alors les inconnues.

(1) La symétrie *verticale*, qui est moins dangereuse pour la sécurité des dépêches, a pour cause la lecture de la *clé* dans l'alphabet normal.

Exemple : Formons la bande (A) avec l'alphabet :

K P Z J U E O Y I T D N X H S C M W G R B L V F Q A

et la bande (B) avec l'alphabet normal et nous pourrons, sans difficulté, traduire le cryptogramme que M. de Calbiac a publié dans *L'Avenir Militaire*, numéro 2056 du 6 décembre 1895, commençant par :

XY YN EC GJ GP TX TL IL DO KS HA MY FB NA
LG VP TX SZ GT ZZ KX ..

Le premier groupe est insuffisamment déterminé, cependant son deuxième signe Y prouve que la première lettre claire est placée, dans l'alphabet normal, *sept* rangs après la deuxième claire ; le contexte nous fixera sur la valeur de ces deux lettres.

Les autres groupes se traduiront en amenant, comme l'indiquent les diagrammes ci-dessus, la dernière lettre du premier groupe Y au niveau de la première du second Y ; au niveau de la dernière lettre du deuxième groupe N, nous lirons la première claire et, au niveau de K, origine de l'alphabet (A), nous trouverons la deuxième claire ; et ainsi des autres groupes :

1er	2e	3e	4e	5e	6e	7e	8e	9e	10e
K -	K *r*	K *t*	K *r*	K *d*	K *s*	K *h*	K *n*	K *i*	K *e*
: :	: :	: :	: :	: :	: :	: :	: :	: :	: :
- X	Y Y	N E	C G	J G	P T	X T	L I	L D	O K
: :	: :	: :	: :	: :	: :	: :	: :	: :	: :
Y -	N *c*	C *i*	J *u*	P *e*	X *e*	L *c*	L *i*	O *o*	S *s*

La traduction sera donc : *L'écriture des Chinois est un système de signes qui...*

Il semble superflu de s'appesantir sur ce sujet ; nous allons donc entreprendre l'étude des *grilles chiffrantes* et des résultats remarquables qu'elles sont susceptibles de fournir.

Grilles chiffrantes. — Ces grilles sont, comme les autres, formées d'une plaque mince, que nous supposons quadrillée d'un côté, et dont quelques carrés ont été découpés à jour pour déterminer des *fenêtres* ou *ouvertures*.

La grille proprement dite, ou *grille centrale*, formant un carré parfait, a autant de rangées horizontales que de colonnes verticales. On perce une fenêtre dans chaque colonne, en ayant soin que ces fenêtres se trouvent sur des rangées différentes, de telle sorte que, dans toutes les positions de la grille, il y ait une fenêtre et une *seule* dans chaque colonne.

Entre le bord de la grille centrale et l'extrémité de la plaque,

on laisse une bordure de largeur variable, qui diffère pour chaque côté.

Sous une grille ainsi formée, disposons un nombre suffisant de bandes alphabétiques, puis, faisant glisser les bandes, amenons les lettres du texte à cryptographier sur la ligne immédiatement au-dessus du bord supérieur de la grille : les lettres qui apparaitront aux ouvertures serviront de chiffres. Il n'est pas besoin de faire remarquer que l'intervalle entre deux lettres consécutives d'une bande quelconque doit, ainsi que la largeur de la bande, être égal à la largeur d'une colonne de la grille.

Mouvements de la grille. — En faisant tourner la grille à angle droit, on lui donne *quatre* positions différentes ; en la rabattant ensuite de manière à mettre sa face supérieure en dessous, on obtient, par rotation, *quatre* nouvelles positions, soit *huit* en tout.

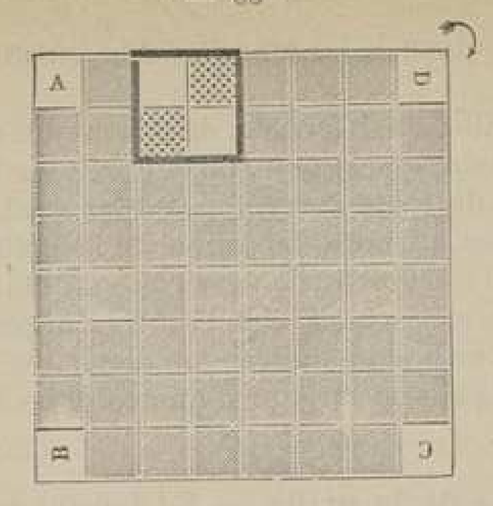
Ce nombre est doublé et porté à *seize* en posant la grille *au-dessus* du texte clair, après l'avoir placée *au-dessous*, ce qui transforme les clés positives en clés négatives.

Roulement des alphabets. — Les alphabets, après avoir servi à un chiffrement partiel, sont, au moment fixé par les conventions, reportés l'un après l'autre de gauche à droite ou de droite à gauche, ce qui fournit autant de groupes qu'il y a d'alphabets et porte le total des alphabets utilisés, en tenant compte des mouvements de la grille, à $16\,n^2$, en indiquant par n le nombre des bandes employées.

Si considérable qu'il soit, ce nombre peut être notablement augmenté sans que cela entraine de grandes complications. Ainsi quatre bandes pouvant se grouper de vingt-quatre manières différentes, le nombre ci-dessus devrait, dans le cas de $n = 4$, être multiplié par 6, ce qui, au lieu de $16 \times 4^2 = 256$ alphabets, en donnerait $16 \times 4^2 \times 6 = 1.536$. Pour cinq bandes, on aurait 9.600 alphabets.

Il est vrai que, dans la pratique, ces nombres ne peuvent être atteints, néanmoins le nombre des clés et des alphabets utilisables est tellement considérable qu'aucune autre méthode alphabétique ne peut offrir autant de garanties que celle des grilles chiffrantes, qui présente, en outre, la plus grande facilité d'emploi.

Application. — Appliquons la méthode dont l'exposé précède au cas le plus simple, c'est-à-dire à *deux* bandes avec une grille à *deux* ouvertures ayant la forme indiquée ci-après :



Sur trois des côtés de la *grille centrale*, on a laissé des marges respectivement égales à une, deux et trois fois la largeur de la grille, ce qui permettra de prendre pour chiffres, sur chaque bande, les lettres distantes des claires de un, deux, trois... huit intervalles.

Prenons deux bandes alphabétiques, A, B : faisons-les glisser pour amener au bord supérieur de l'appareil les deux premières lettres du texte à cryptographier et prenons pour chiffres les lettres qui apparaitront aux fenêtres de la grille. Le premier chiffre, que nous représenterons par A_1, sera donc la lettre qui, dans l'alphabet A, suit la claire immédiatement, c'est-à-dire à *un* intervalle ; le second chiffre, B_2, est la lettre qui, dans l'alphabet B, suit la claire à *deux* intervalles.

Donnons ensuite aux bandes alphabétiques la position BA et nous chiffrerons avec B_1 et A_2.

Le report à droite de la bande de gauche ramenant la position primitive, AB, nous faisons tourner la grille d'un angle droit, de manière à remplacer la lettre *a* de la grille par la lettre *b* et nous chiffrons comme précédemment, mais alors les alphabets employés sont A_4, B_3, puis B_4, A_3.

Les deux autres mouvements de la grille, joints au transport des bandes de gauche à droite, mettront à notre disposition les alphabets A_7, B_8 — B_7, A_8 — A_6, B_5 — B_6, A_5.

Toutes les positions respectives de la grille et des bandes étant épuisées, nous retournons la grille, la face supérieure en dessous, par exemple de manière que a prenne la place de *d*, et *b* celle de c, et nous recommençons à chiffrer comme ci-dessus.

Les alphabets successivement employés sont : A_2 B_1 B_2 A_1 — A_5 B_6 B_5 A_6 — A_8 B_7 B_8 A_7 — A_3 B_4 B_3 A_4.

Le tableau suivant présente l'ensemble des résultats obtenus :

	A	B	B	A	A	B	B	A	A	B	B	A	A	B	B	A
Grille normale :	1	2	1	2	4	3	4	3	7	8	7	8	6	5	6	5
Grille retournée :	2	1	2	1	5	6	5	6	8	7	8	7	3	4	3	4

Nous avons donc chiffré trente-deux lettres, sans que deux alphabets se reproduisent dans les mêmes conditions. Si maintenant nous employons les clés négatives, en mettant la grille *au-dessus* du texte clair, nous trouverons trente-deux nouveaux chiffres ne présentant encore aucune répétition.

Deux bandes alphabétiques, ainsi employées, donnent donc des résultats qu'on ne pourrait obtenir qu'avec *cinquante-deux* alphabets différents et une clé de soixante-quatre lettres. *Trois* bandes alphabétiques et une grille à *trois* ouvertures peuvent fournir les mêmes résultats que *soixante-dix-huit* alphabets avec une clé de cent quarante-quatre lettres ; *quatre* bandes équivalent à *cent quatre* alphabets avec une clé de deux cent cinquante-six ; *cinq* bandes ont la valeur de *cent trente* alphabets différents avec une clé de quatre cents lettres, etc.

Pour doubler l'importance de la clé (le cas de deux bandes excepté), il suffit, à la fin de la période, de renverser l'ordre primitivement donné aux alphabets et de prendre pour nouveau point de départ M L K... C B A, au lieu de A B C... K L M. Dans ces conditions, *cinq* bandes alphabétiques équivaudraient à *cent trente* alphabets employés avec une clé de huit cents lettres.

On voit quelles immenses ressources les *grilles chiffrantes* offrent aux cryptographes : entre des mains exercées, ces ressources sont presque inépuisables.

Dans la pratique courante, il est inutile de poursuivre toutes les combinaisons possibles : un petit nombre de mouvements de la grille, joint au roulement des alphabets, fournit une clé de longueur suffisante pour déjouer toutes tentatives de déchiffrement. Mais il importe que les conventions fixent bien la marche à suivre, tant pour cryptographier que pour traduire.

Exemple. — Soit à traduire la dépêche :

(1) LIPGO CQYXG UGRCC BRPQZ ZGOG

Les correspondants étant supposés en possession d'une série de vingt-cinq alphabets intervertis, disposés en bandes et débutant chacun par une lettre différente, *le mot d'ordre* BARIL, suffit pour leur faire connaître les bandes à employer et l'ordre de ces bandes.

L'ordre alphabétique des lettres du mot BARIL fournit la série : 21534, qui servira à la confection de la grille.

Pour plus de clarté et rien ne s'y opposant dans le cas actuel, nous découperons dans une feuille de carton convenablement quadrillé, une grande fenêtre, réservée au texte clair et laissant lire cinq lettres consécutives. Dans la première colonne, c'est-à-

(1) Ce cryptogramme fait partie de ceux, en grande partie traduits, que *L'Avenir Militaire*, dans son numéro 2073, du 4 février 1896, a offert à la sagacité de ses lecteurs, en invitant les cryptophiles à combler les petites lacunes que présentaient les traductions.

dire celle qui contient la première lettre du texte, nous éviderons le deuxième carré de manière à découvrir la lettre qui se trouve au deuxième rang au-dessus du clair; dans la deuxième colonne, nous éviderons le carré qui masque la lettre immédiatement au-dessus du clair; enfin, dans les troisième, quatrième et cinquième colonnes, nous disposerons les ouvertures de telle sorte qu'elles découvrent les lettres situées respectivement aux cinquième, troisième et quatrième rangs au-dessus de celles qui apparaitront dans la grande fenêtre. La grille, ainsi formée, laissera donc lire les lettres placées sur les bandes à deux, un cinq, trois, quatre rangs du texte clair, comme le prescrit la clé.

Le mouvement de la grille a été limité, par convention, à deux positions :

Dans la première, les *chiffres* se trouvent *au-dessus du clair*, dans l'ordre et aux distances déterminés par la clé;

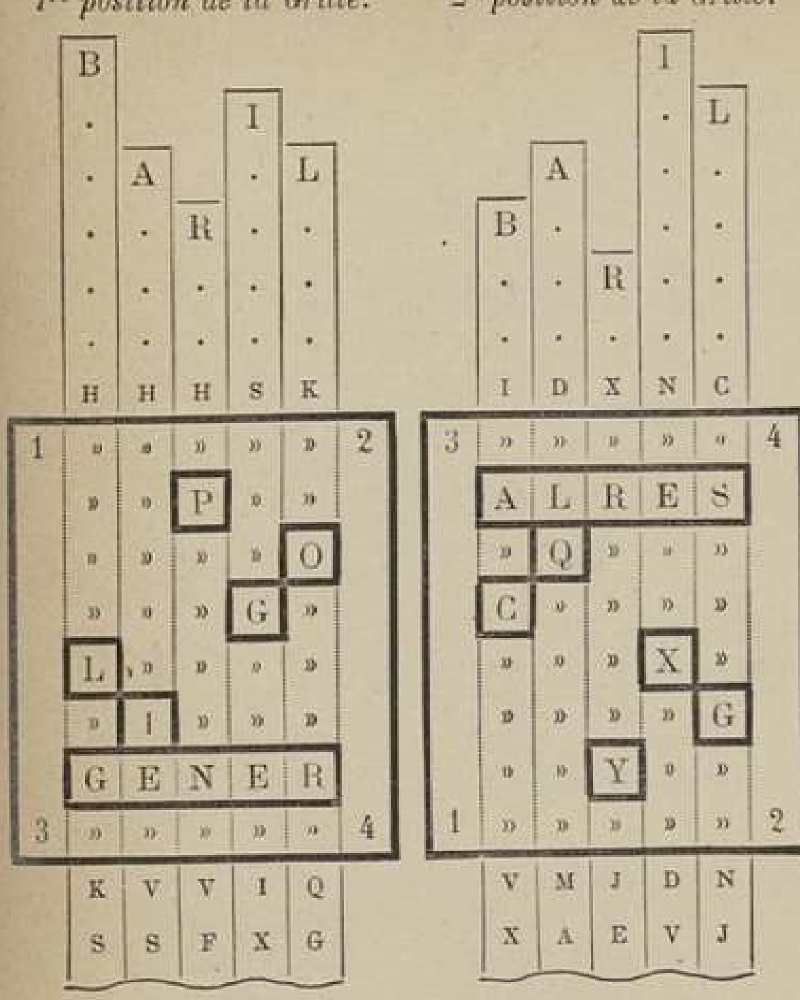
Dans la deuxième, qui s'obtient par le rabattement de la grille, *sans rotation*, la grande fenêtre se trouve au-dessus des petites, qui en sont distantes de deux, un, cinq, trois, quatre rangs.

Enfin, il est convenu que chaque double mouvement de la grille sera suivi du déplacement de la première bande, laquelle sera reportée de gauche à droite. Le roulement des alphabets fournira ainsi cinq groupes successifs : BARIL, ARILB, RILBA, ILBAR, LBARI, qui, avec les deux positions de la grille donneront une clé *automatique* de cinquante alphabets secondaires, savoir :

Alphabets primaires :	A	B	I	L	R
Clés numériques déterminant les alphabets secondaires :	25	24	23	22	21
	1	2	3	4	5
	24	22	21	23	25
	2	4	5	3	1
	22	23	25	21	24
	4	3	1	5	2
	23	21	24	25	22
	3	5	2	1	4
	21	25	22	24	23
	5	1	4	2	3

Le cryptogramme qui nous occupe n'ayant que dix-neuf lettres, chacune a été chiffrée avec un alphabet différent, ce qui le rend inviolable, aucune répétition ne pouvant guider les recherches du déchiffreur.

Les diagrammes ci-contre font ressortir clairement la manœuvre de la grille et des réglettes dans le chiffrement de la dépêche. La traduction pourrait s'effectuer par une position *inverse* de la grille, mais cette méthode, qui offre quelques inconvénients, ne présente pas d'avantages réels.



1re position des Alphabets.
1re position de la Grille.

1re position des Alphabets.
2e position de la Grille.

2e position des Alphabets
1re position de la Grille.

		R				
		B				
		H		L		
		T		N		
		P		J	B	
		Y	I	A	K	
	A	S	X	Y	S	
	F	J	M	U	D	
	J	E	P	P	O	
	Z	N	A	E	J	
	X	Q	D	H	T	
	B	V	V	Z	R	
	P	F	Y	B	F	
	G	K	L	X	P	
	R	U	Q	M	I	
	K	C	H	K	Y	
1	C	M	K	V	A	2
	N	I	R	F	Z	
	Y	Z	B	O	C	
	H	D	F	C	U	
	U	O	J	I	Q	
	D	G	S	S	H	
	T	A	U	R	E	
3	L	X	T	T	V	4
	Q	L	Z	Q	X	
	I	R	G	G	M	
	E	B	N	D	L	
	O	H	C	L	N	
	V	T	E	N	G	
	S	P	O	J	B	
	M	Y	I	A	K	
	A	S	X	Y	S	
	F	J	M	U	D	
	J	E	P	P	O	
	Z	N	A	E	J	

2e position des Alphabets.
2e position de la Grille.

	A	R	I	L	B	
	.	.	.	.	.	
	.	.	.	.	.	
	A	G	G	O	T	
3	»	»	»	»	»	4
	Z	L	E	S	P	
	»	R	»	»	»	
	B	»	»	»	»	
	»	»	»	Q	»	
	»	»	»	»	Z	
	»	»	P	»	»	
1	»	»	»	»	»	2
	K	Y	A	L	U	
	C	S	D	N	Q	

3e position des Alphabets.
1re position de la Grille.

	R	I	L	B	A	
	.	.	.	.	.	
	.	.	.	.	.	
	F	B	K	V	»	
1	»	»	»	»	»	2
	»	»	O	»	»	
	»	»	»	»	»	
	»	»	»	G	»	
	Z	»	»	»	»	
	»	G	»	»	»	
	O	N	T	S	»	
3	»	»	»	»	»	4
	L	I	L	O	»	
	R	X	N	J	»	

TROISIÈME PARTIE

SUBSTITUTION COMPLEXE

Polygrammes.

Le chiffrement par *polygrammes* est caractérisé par ce fait que *toutes les lettres d'un groupe participent à la détermination de chacun des chiffres composant le cryptogramme correspondant*.

Eclaircissons ceci par un exemple :

Si nous supposons que A a une valeur représentée par 123, que B = 456 et C = 789, nous pourrons cryptographier le groupe ABC en prenant à A l'un des chiffres 1, 2 ou 3, à B 4, 5 ou 6 et à C 7, 8 ou 9 ; l'ensemble des premiers trois chiffres choisis, soit, si l'on veut 147, sera la valeur de la première lettre du trigramme cryptographié, 258 pourra être la valeur de la deuxième, et 369 celle de la troisième.

On voit que chaque lettre claire intervient pour un tiers dans la détermination de chacune des lettres formant cryptogramme et, par conséquent, qu'aucune méthode alphabétique ne pourra donner les mêmes chiffres pour les mêmes groupes de lettres claires.

Aucun auteur, que nous sachions, n'a parlé du chiffrement par polygrammes avant la brochure que nous avons publiée en 1893, où la nouvelle méthode est exposée (1).

Les méthodes dites à bigrammes et à trigrammes, mentionnées par Blaise de Vigenère et Gustave Selenus, ne satisfont pas à la définition donnée plus haut et ne sont, en effet, comme celle de M. de Calbiac (page 63), que des applications des méthodes alphabétiques avec autochiffrement.

(1) *Cryptographie nouvelle*, Paris, Dubreuil, éditeur.

Les *polygrammes* se subdivisent en *bigrammes* et *trigrammes*. Les polygrammes d'un ordre plus élevé ne paraissent pas susceptibles d'entrer dans la pratique de la cryptographie; cependant les *hexagrammes* pourront rendre quelques services.

Les polygrammes sont dits *fixes* ou *entiers*, lorsque chaque groupe de lettres claires est toujours cryptographié par le même groupe de chiffres.

Ils sont *scindés* ou *variables*, lorsqu'une des lettres claires, après s'être combinée avec une ou plusieurs autres pour déterminer un premier chiffre, s'associe à d'autres claires pour former de nouveaux cryptogrammes.

Ayant à chiffrer A, B, C, D, E..... nous emploierons un trigramme *fixe* si nous substituons à ABC les chiffres *xyz*; nous ferons, au contraire usage de trigrammes scindés si, après avoir déduit *x* de ABC, nous déduisons *u* de ADF, et *v* de AGK, ce qui s'obtiendra facilement et, pour ainsi dire mécaniquement, sans effort ni tension d'esprit.

Les polygrammes *fixes* sont *rompus* ou *fractionnés*, lorsque les chiffres qui les composent sont disjoints au lieu de former un groupe dans le cryptogramme.

Nous commencerons l'étude des polygrammes par les *bigrammes* et nous l'achèverons par les *trigrammes* et les *hexagrammes*.

Bigrammes.

Bigrammes fixes.— Le moyen, en apparence, le plus simple d'obtenir les bigrammes *fixes* consiste à combiner méthodiquement deux à deux toutes les lettres de l'alphabet, puis après avoir interverti leur ordre de succession ou séquence, à rapprocher cette liste d'une autre liste *normale* présentant tous les bigrammes dans l'ordre alphabétique: AA, AB, AC .... AZ, BA, BB..... BZ, CA, CB, etc.

La longueur de ces listes comprenant chacune six cent vingt-cinq ou six cent soixante-seize groupes, suivant que l'alphabet employé est de vingt-cinq ou de vingt-six lettres, et la nécessité d'établir une liste *chiffrante* et une liste *déchiffrante* rendent ce système peu pratique.

En inscrivant, au contraire, les bigrammes sur un tableau à deux entrées, disposé exactement comme le chiffre carré de Vigenère, les recherches deviennent faciles et le chiffrement beaucoup plus rapide qu'avec les carrés alphabétiques, chaque case fournissant *deux* lettres au lieu *d'une*. Mais, si l'on veut éviter l'emploi de deux tableaux, l'un *chiffrant* et l'autre *déchiffrant*, il est indispensable de rendre le tableau *réciproque*, c'est-à-dire tel que si on a AZ = *os*, on ait aussi OS = *az*.

Le tableau ci-après a été construit dans ces conditions, il peut donc servir indifféremment au chiffrement et à la lecture.

Il importe de remarquer que, ces tableaux n'étant pas symétriques, chaque entrée est *exclusivement* affectée à la première ou à la deuxième lettre du groupe à cryptographier. Dans le tableau qui suit, la première lettre à chiffrer doit se lire dans l'alphabet vertical et la deuxième dans l'alphabet horizontal ; le bigramme cryptographique se trouve dans le carré appartenant, à la fois, à la *rangée de la première lettre* et à la *colonne de la deuxième*.

Pour cryptographier à l'aide de ce tableau, après avoir divisé le texte en groupes de *deux* lettres, on cherche le bigramme correspondant à chaque groupe en lisant, comme nous l'avons dit, la première lettre claire dans l'alphabet vertical et la deuxième dans l'alphabet horizontal.

Soit, par exemple, à *bigraphier*.

La société humaine se compose de familles et non d'individus.

Le premier groupe, *la*, se traduira par HQ ; le deuxième, *so*, par ZL ; le troisième, *ci* par GD, etc. ; ainsi que l'indique le diagramme ci-après :

la so ci et eh um ai ne se co mp os ed ef am il
HQ ZL GD BI SL UG VS OP HL JN NR AZ FI FJ XG VH

le se tn on di nd iv id us
HP HL MR TE IU MY XB MI UC

et on aura pour cryptogramme : HQZLGDBISLUGVSOPHLJN NRAZFIFJXGVHHPHLMRTEIUMYXBMIUC.

Pour la traduction, on opèrera exactement de la même manière que pour le chiffrement : cherchant le premier chiffre de chaque groupe dans l'alphabet vertical et le deuxième dans l'alphabet horizontal, on trouve à l'intersection des deux lignes le bigramme clair : HQ = *la*, ZL = *so*, GD = *ci*.....

Ainsi établi, un cryptogramme d'une longueur moyenne est absolument indéchiffrable pour celui qui ne possède pas le tableau servant au chiffrement.

Il n'en est plus tout à fait ainsi lorsque le déchiffreur ennemi a pu réunir un grand nombre de dépêches bigraphiées avec le *même* tableau ou lorsque le cryptogramme est d'une longueur suffisante pour que les bigrammes clairs les plus fréquemment employés, tels que : *es, en, le, de, on, ou, nt, re, ed*..... sont répétés assez de fois pour guider les recherches.

On peut obvier à cet inconvénient en *rompant* ou *fractionnant* les bigrammes chiffrés, ou en groupant les lettres claires dans un ordre autre que celui de l'écriture.

Tableau des bigrammes

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
A	OV	VV	XS	MC	OG	MS	XM	VG	VS	VC	MV	VM	XG	MM	DG
B	HA	EA	QT	KZ	HX	KT	QE	EX	ET	EZ	KA	EE	QX	KE	ZX
C	RK	GK	UD	CF	RN	CD	UR	GN	GD	GF	CK	GR	UN	CR	JN
D	YQ	IQ	AU	TY	YP	TU	AO	IP	IU	IY	TQ	IO	AP	TO	NP
E	BB	SB	PJ	FI	BL	FJ	PH	SL	SJ	SI	FB	SH	PL	FH	LL
F	HK	EK	QD	KF	HN	KD	QB	EN	ED	EF	KK	ER	QN	KR	ZN
G	RB	GB	UJ	CI	RL	CJ	UH	GL	GJ	GI	CB	GH	UL	CH	JL
H	BA	SA	PT	FZ	BX	FT	PE	SX	ST	SZ	FA	SE	PX	FE	LX
I	OB	VB	XJ	MI	OL	MJ	XH	VL	VJ	VI	MB	VH	XL	MH	DL
J	RQ	GQ	UU	CY	RP	CU	UO	GP	GU	GY	CQ	GO	UP	CO	JP
K	BK	SK	PD	FF	BN	FD	PR	SN	SD	SF	FK	SR	PN	FR	LN
L	HQ	EQ	QU	KY	HP	KU	QO	EP	EU	EY	KQ	EO	QP	KO	ZP
M	YK	IK	AD	TF	YN	TD	AR	IN	ID	IF	TK	IR	AN	TR	NN
N	OQ	VQ	XU	MY	OP	MU	XO	VP	VU	VY	MQ	VO	XP	MO	DP
O	YA	IA	AT	TZ	YX	TT	AE	IX	IT	IZ	TA	IE	AX	TE	NX
P	HV	EV	QS	KC	HG	KS	QM	EG	ES	EC	KV	EM	QG	KM	ZG
Q	BV	SV	PS	FC	BG	FS	PM	SG	SS	SC	FV	SM	PG	FM	LG
R	RA	GA	UT	CZ	RX	CT	UE	GX	GT	GZ	CA	GE	UX	CE	JX
S	HB	EB	QJ	KI	HL	KJ	QH	EL	EJ	EI	KB	EH	QL	KH	ZL
T	OK	VK	XD	MF	ON	MD	XR	VN	VD	VF	MK	VR	XN	MR	DN
U	RV	GV	US	CC	RG	CS	UM	GG	GS	GC	CV	GM	UG	CM	JG
V	YB	IB	AJ	TI	YL	TJ	AH	IL	IJ	II	TB	IH	AL	TH	NL
X	YV	IV	AS	TC	YG	TS	AM	IG	IS	IC	TV	IM	AG	TM	NG
Y	OA	VA	XT	MZ	OX	MT	XE	VX	VT	VZ	MA	VE	XX	ME	DX
Z	BQ	SQ	PU	FY	BP	FU	PO	SP	SU	SY	FQ	SO	PP	FO	LP
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O

disposés en chiffre carré.

P	Q	R	S	T	U	V	X	Y	Z	
DM	DV	MG	XC	OC	DC	XV	OM	DS	OS	A
ZE	ZA	KX	QZ	HZ	ZZ	QA	HE	ZT	HT	B
JR	JK	CN	UF	BF	JF	UK	RB	JD	RD	C
NO	NQ	TP	AY	YY	NY	AQ	YO	NU	YU	D
LH	LB	FL	PI	BI	LI	PB	BH	LJ	BJ	E
ZR	ZK	KN	QF	HF	ZF	QK	HR	ZD	HD	F
JH	JB	CL	UI	RI	JI	UB	RH	JJ	RJ	G
LE	LA	FX	PZ	BZ	LZ	PA	BE	LT	BT	H
DH	DB	ML	XI	OI	DI	XB	OH	DJ	OJ	I
JO	JQ	CP	UY	RY	JY	UQ	RO	JU	RU	J
LR	LK	FN	PF	BF	LF	PK	BR	LD	BD	K
ZO	ZQ	KP	QY	HY	ZY	QQ	HO	ZU	HU	L
NR	NK	TN	AF	YF	NF	AK	YR	ND	YD	M
DO	DQ	MP	XY	OY	DY	XQ	OO	DU	OU	N
NE	NA	TX	AZ	YZ	NZ	AA	YE	NT	YT	O
ZM	ZV	KG	QC	HC	ZC	QV	HM	ZS	HS	P
LM	LV	FG	PC	BC	LC	PV	BM	LS	BS	Q
JE	JA	CX	UZ	RZ	JZ	UA	RE	JT	RT	R
ZH	ZB	KL	QI	HI	ZI	QB	HH	ZJ	HJ	S
DR	DK	MN	XF	OF	DF	XK	OR	DD	OD	T
JM	JV	CG	UC	RC	JC	UV	RM	JS	RS	U
NH	NB	TL	AI	YI	NI	AB	YH	NJ	YJ	V
NM	NV	TG	AC	YC	NC	AV	YM	NS	YS	X
DE	DA	MX	XZ	OZ	DZ	XA	OE	DT	OT	Y
LO	LQ	FP	PY	BY	LY	PQ	BO	LU	BU	Z
P	Q	R	S	T	U	V	X	Y	Z	

Bigrammes rompus. — Pour *rompre* les bigrammes, au lieu d'écrire horizontalement, côte à côte, les chiffres qui les composent, on écrit ceux-ci verticalement, le deuxième au-dessous du premier :

```
H Z G B S U ....
Q L D I L G ....
```

puis on les relève par groupes d'une longueur fixée par les conventions.

Soit dix, la base du groupement choisi, le cryptogramme ci-dessus deviendra : HZGBSUVOHJQLDILGSPLNNAFFXVH HMTRZIJGHPLREIMXMUUYBIC, et, par suite de la transposition, le bigramme HL, qui figure deux fois dans le premier cryptogramme, n'est plus apparent dans celui-ci.

Il est évident que tous les relevés étudiés dans les méthodes de transposition sont applicables aux bigrammes, mais il importe d'éviter les complications.

Pour décomposer les bigrammes de l'écriture usuelle, il suffit d'écrire sur deux lignes le texte à cryptographier et de chiffrer ensemble les lettres de *même rang* sur les deux lignes :

```
l a s o c i e t e h u m a i n e s e c o m p o s e
d e f a m i l l e s e t n o n d i n d i v i d u s
K O K Y U V S V B P R Y M D M F E F C I A E T Z P
Y G J A N J H R L Z G F M L O I J H F T K S Z I I
```

En relevant la ligne des premiers chiffres et la faisant suivre de celle des seconds, chaque chiffre occupe, dans le cryptogramme, le même rang que, dans le texte clair, une des lettres qui lui a donné naissance.

En séparant la dépêche par groupes d'une longueur déterminée par les conventions et en faisant suivre la première ligne des chiffres de chaque groupe par la seconde du même groupe, on *transpose* ces groupes en entremêlant les deux lignes du clair.

Enfin, si on écrit horizontalement tous les bigrammes-chiffres, au fur et à mesure qu'ils sont formés, cela revient à mélanger, lettre à lettre, les deux lignes du clair; le cryptogramme ci-dessus deviendrait alors : KYOGKJYAUNVJSHVRBLPZRG YFMMDLMOFIEJFHCFITAKESTZZIPI.

Ces procédés simples et d'une application facile, n'entraînent de difficultés ni pour le chiffrement, ni pour la lecture, lorsque les conventions sont bien établies; mais la formation du tableau des bigrammes est longue et laborieuse, surtout pour obtenir la réciprocité et éviter la construction de deux tableaux, l'un chiffrant et l'autre déchiffrant. Il importait donc de découvrir un procédé, simple et pratique, permettant de supprimer ces tableaux, comme les bandes alphabétiques permettent de supprimer les tableaux de Vigenère et de Beaufort.

Après de longues recherches, nous avons trouvé la solution de ce problème et imaginé deux procédés satisfaisant à ce *desideratum* : les *damiers bigrammatiques* et les *alphabets bifides* ou *à deux chiffres.*

Damiers bigrammatiques et carrés alphabétiques. — Un *carré alphabétique simple* consiste en un damier de vingt-cinq cases, dont chacune contient dans un ordre déterminé, l'une des lettres de l'alphabet normal. La réunion de quatre de ces carrés constitue un *damier bigrammatique complet.*

Voici le damier bigrammatique qui a servi à la construction du tableau de la page 74 :

	Q	H	K	Z	E	f	s	b	p	l	
	A	Y	T	N	I	m	v	o	x	d	
1	P	B	F	L	S	k	e	h	q	z	2
	U	R	C	J	G	c	g	r	u	j	
	X	O	M	D	V	t	i	y	a	n	
	g	x	n	p	l	R	H	E	M	O	
	v	a	k	q	b	K	B	A	V	Q	
4	s	t	d	u	j	F	I	Z	C	Y	3
	m	e	r	o	h	N	L	X	G	P	
	c	z	f	y	i	D	J	T	S	U	

Les quartiers un et trois écrits en capitales, renferment les alphabets *principaux* et les deux autres quartiers contiennent les alphabets *auxiliaires.*

Pour faire usage de ce damier, on cherche les lettres claires dans les alphabets principaux, en prenant la première dans le quartier numéro un et la deuxième dans le quartier numéro trois. Ces deux lettres étant supposées aux extrémités de la diagonale d'un parallélogramme rectangle, ce parallélogramme est entièrement déterminé et les lettres qui se trouvent, dans les alphabets auxiliaires, aux extrémités de l'autre diagonale, forment le bigramme cherché, dont le premier chiffre se lit dans le quartier numéro deux et le deuxième dans le quartier numéro quatre.

Pour faciliter les recherches, il est commode de se servir de deux cartons évidés à angle droit. On fait glisser ces sortes d'équerres le long des lignes du damier et on amène chaque lettre claire dans l'angle de l'un de ces cartons, dont les côtés,

en se rejoignant, délimitent le parallélogramme et mettent en évidence les lettres formant le chiffre.

Dans le diagramme qui précède, on a indiqué par des lignes ponctuées la position des deux équerres pour le chiffrement de CH = *gn*.

Lorsque le damier bigrammatique possède les qualités qui assurent la réciprocité ou le renversement, la traduction s'opère exactement comme le chiffrement, en lisant les chiffres à traduire dans les alphabets principaux et leur valeur dans les auxiliaires.

Lorsque la réciprocité n'existe pas et que, par suite, le renversement n'est pas possible, la lecture ne peut se faire qu'en cherchant les chiffres dans les alphabets auxiliaires, les principaux étant exclusivement réservés aux lettres claires.

Conditions assurant la réciprocité. — En examinant le diagramme qui précède, on voit que le premier chiffre du bigramme se trouve à l'intersection de la ligne horizontale, ou rangée, qui contient la première lettre claire et de la ligne verticale, ou colonne, qui renferme la deuxième claire. De même, le deuxième chiffre du bigramme est à la rencontre de la colonne de la première claire et de la rangée de la deuxième.

Pour que le renversement soit possible et qu'il y ait réciprocité, il est donc indispensable que les rangées des alphabets principaux contenant les chiffres obtenus précédemment soient complétées par les lettres claires de la première position; il en est de même des colonnes.

Le diagramme ci-après mettra ce fait en évidence :

		1	2	3	4	5	3	5	2	1	4		
	1	Q	H	K	Z	E	f	s	b	p	l	3	
	2	·	Y	·	N	·	·	·	o	·	d	5	
1	3	P	B	F	L	S	k	e	h	q	z	1	2
	4	·	R	·	J	·	·	·	r	·	j	4	
	5	·	O	·	D	·	·	·	y	·	n	2	
	4	g	x	n	p	l	R	H	E	M	O	1	
	2	·	a	·	q	·	·	·	A	·	Q	2	
4	5	·	t	·	u	·	·	·	Z	·	Y	3	3
	1	m	e	r	o	h	N	L	X	G	P	4	
	3	·	z	·	y	·	·	·	T	·	U	5	
		4	3	1	5	2	1	2	3	4	5		

D'après le mode d'emploi du damier, tout bigramme clair *commençant* par une des lettres : P, B, F, L, S, aura pour premier chiffre l'une des lettres : *k, e, h, q, z*, qui se trouvent sur la même rangée.

De même, tout bigramme clair *finissant* par une des lettres : E, A, Z, X, T, aura pour premier chiffre l'une des lettres : *b, o, h, r, y*, qui se trouvent dans la même colonne.

Par suite, *seuls*, les vingt-cinq bigrammes clairs *commençant* par une des lettres : P, B, F, L, S, et *se terminant* par : E, A, Z, X ou T, auront *h* pour premier chiffre.

On voit facilement que, pour les mêmes raisons, *seuls*, les vingt-cinq bigrammes clairs *commençant* par une des lettres : Z, N, L, J, D, et *se terminant* par R, H, E, M ou O, auront *p* pour second chiffre.

Or, *seul*, le groupe LE appartient aux deux séries, donc il pourra, *seul*, être chiffré par le bigramme *h p*.

Pour qu'il y ait réciprocité, il faut que, si les lettres P, B, F, L, S, formant une rangée du premier alphabet principal, peuvent être chiffrées par une des lettres *k, e, h, q, z*, du premier alphabet auxiliaire, ces dernières lettres forment une rangée de l'alphabet principal et soient suivies, dans l'alphabet auxiliaire, des lettres *p, b, f, l, s*, dans un ordre quelconque; en d'autres termes, si la troisième rangée du premier alphabet principal est suivie de la première du même alphabet, la première devra être suivie de la troisième. Le deuxième alphabet principal est astreint à la même loi, sans qu'il en résulte, pour cela, une dépendance quelconque entre les moitiés supérieure et inférieure du damier.

La seconde condition de réciprocité, c'est que les colonnes verticales de la partie droite du damier soient constituées des mêmes éléments, dans un ordre quelconque, que celles de la partie gauche; c'est-à-dire que si une colonne entière est formée, par exemple, de la deuxième colonne du premier alphabet principal et des lettres appartenant à la troisième colonne du second alphabet principal, la troisième colonne de ce dernier alphabet doit être surmontée des lettres appartenant à la deuxième colonne du premier alphabet principal.

En résumé, les deux conditions nécessaires et suffisantes de la réciprocité consistent :

1° Dans la formation des alphabets *auxiliaires* par la permutation *réciproque* des *rangées* de chacun des alphabets principaux;

2° Dans l'*identité* des éléments constituant les *colonnes* des deux moitiés verticales du damier.

La permutation réciproque de *cinq* rangées peut se faire de vingt-six manières différentes, soit, pour deux carrés indépendants, 26 × 26 = 676 combinaisons. D'autre part, le nombre des

arrangements que peuvent prendre les cinq colonnes s'élève à $5 \times 4 \times 3 \times 2 \times 1 = 120$. Nous pouvons donc, avec deux alphabets principaux donnés, former $676 \times 120 = 81.120$ damiers bigrammatiques jouissant de la réciprocité. Quant au nombre de ceux dépourvus de cette propriété, il excède les limites du calcul.

Damiers bigrammatiques réduits. — Lorsque, dans un damier complet, le quatrième carré est identique au premier et le deuxième identique au troisième, on peut supprimer la moitié inférieure du damier et obtenir les mêmes bigrammes qu'avec le damier complet.

	A	B	C	D	E	H	A	T	N	X	
	F	G	H	I	J	E	B	V	I	L	
1	K	L	M	N	O	G	Q	S	O	D	2
	P	Q	R	S	T	C	J	U	M	F	
	U	V	X	Y	Z	Z	Y	R	P	K	

Pour bigraphier avec un damier réduit à ses deux alphabets principaux placés horizontalement, on cherche la première lettre du groupe clair dans le premier alphabet et la deuxième dans le second; le premier chiffre se lit dans *la colonne de la deuxième claire* et le deuxième dans *la colonne de la première,* toujours au niveau de l'autre lettre claire. On trouve ainsi : NN=*od*, IO=*in*, LU=*sq*, OS=*so*..... etc.

Proposons-nous, par exemple, de bigraphier :

Ni l'or, ni la grandeur ne nous rendent heureux.

Le nombre des lettres à chiffrer étant impair, nous ajouterons une *nulle*, puis, écrivant la phrase sur deux lignes, nous bigraphierons, l'un après l'autre, les groupes formés par les lettres du *même rang*, prises dans chaque ligne :

n i l o r n i l a g r a n d e u r n e
n o u s r e n d e n t h e u r e u x z
O I S S U G I D H I U H G T T Z U D H
D N Q O X I D L F B C A I S Z F R D Z

Nous relèverons ensuite les deux lignes de chiffres, suivant les conventions et de manière à fractionner les bigrammes.

Au lieu d'ajouter une *nulle*, nous aurions pu ne pas chiffrer l'une des lettres, soit celle du commencement, celle du milieu ou celle de la fin; c'est aux conventions à préciser ce point.

La traduction s'opérera comme le chiffrement, en ayant soin toutefois de chercher le premier chiffre dans le deuxième alpha-

bet et le deuxième dans le premier, car ce demi-damier ne jouit pas de la réciprocité.

On pourrait cependant la lui donner par la permutation réciproque des rangées du premier alphabet, l'ordre des colonnes étant quelconque.

La réciprocité reparait dans les *demi-damiers verticaux*.

Lorsque, dans un damier complet, le deuxième carré est identique au premier et le quatrième identique au troisième, on peut supprimer une des moitiés verticales du damier et obtenir les mêmes résultats qu'avec le damier complet.

	A	B	C	D	E
	F	G	H	I	J
1	K	L	M	N	O
	P	Q	R	S	T
	U	V	X	Y	Z
	H	A	T	N	X
	E	B	V	I	L
2	G	Q	S	O	D
	C	J	U	M	F
	Z	Y	R	P	K

Pour bigraphier avec un demi-damier vertical, on opère exactement comme avec un demi-damier horizontal, en cherchant la première lettre du groupe clair dans le premier alphabet et la deuxième dans le second; le premier chiffre se lit dans la colonne de la deuxième claire et le deuxième dans la colonne de la première, toujours au niveau de l'autre lettre claire.

Cryptographions : *ordres exécutés*, en fractionnant les bigrammes clairs et rompant les bigrammes chiffrés.

Nous aurons :

o r d r e s e
x e c u t e s
O P A R C P C
X V M U X I D

et le cryptogramme sera :

OPARCPCXVMUXID.

La traduction s'opérera exactement comme le chiffrement, en lisant le premier chiffre dans l'alphabet supérieur et le deuxième dans l'alphabet inférieur, attendu que la réciprocité existe forcément dans tous les demi-damiers verticaux.

Damiers réduits à un carré alphabétique. — Si nous supposons que les deux alphabets constituant un demi-damier sont identiques, nous pouvons, sans aucun inconvénient, supprimer l'un de ces alphabets, et le damier, réduit à un seul carré, fournira les mêmes bigrammes qu'un damier complet composé de quatre carrés semblables; il jouira, en outre, de la réciprocité.

Le mode d'emploi d'un *carré alphabétique* est le même que celui des damiers complets ou réduits. Il importe cependant de faire remarquer que, si les deux lettres à bigraphier se trouvent sur une même rangée, le bigramme cryptographique sera composé des mêmes lettres inversement placées et que, si les lettres claires sont situées dans une même colonne, le groupe sera chiffré par lui-même.

Soit à bigraphier, avec le carré ci-dessous, la phrase : *La lune emprunte sa lumière au soleil.*

D	S	O	G	U
R	A	V	L	E
J	Q	N	H	Y
Z	X	P	F	B
C	K	M	I	T

D'après les conventions supposées, les lettres étant en nombre impair, celle du milieu ne sera pas chiffrée.

l a l u n e e m p r u n t e s a
l u m i è r e a u s o l e i l -
L E V G Y R | E K B A O H | T L G A
L S I T V E | E V O D U V | E T A -

En séparant les bigrammes-chiffres par groupes de *six* et faisant suivre la première ligne de chaque groupe par la deuxième avant de relever le groupe suivant nous aurons le cryptogramme :

LEVGYRLSITVEEKBAOHEVODUVTLGAETA,

dont la traduction n'offrira aucune difficulté au correspondant connaissant les conventions qui ont présidé au chiffrement.

Rectangles alphabétiques. — Il n'est pas indispensable que les lettres de l'alphabet soient disposées en carrés parfaits, il suffit d'en former des rectangles contenant autant de cases qu'il y a de lettres, car aucune de celles-ci ne doit être répétée et toutes les cases doivent être remplies.

Si, à l'alphabet de vingt-cinq lettres, nous ajoutons les dix chiffres, l'ensemble formera trente-cinq signes, que nous pourrons disposer en un rectangle de cinq rangées et sept colonnes, ou de sept rangées et cinq colonnes.

Si, à ce total, nous ajoutons le W, nous pourrons faire, soit un carré de 6×6, soit un rectangle de 3×12, ou de 4×9, et, employés comme nous l'avons fait pour les carrés, ces rectangles fourniront des bigrammes dont les combinaisons pourront être variées à l'infini.

Pour exemple, supprimons de l'alphabet une des lettres les moins employées, soit Z, et convenons que les groupes dont Z fait partie se chiffreront par la simple inversion des lettres de ces groupes : AZ=*za*, BZ=*zb*, ZC=*cz*, ZO=*oz*.... Il restera vingt-quatre lettres, que nous pouvons inscrire dans un rectangle de 3×8 ou de 4×6; choisissons ce dernier et formons deux damiers complets. Nous aurons :

Z	1	2	3	4	5	6	5	3	2	6	1	4	
1	A	J	G	K	N	E	r	c	m	y	f	h	3
2	O	B	T	P	U	I	l	s	x	v	q	d	4
3	F	M	C	H	R	Y	n	g	j	e	a	k	1
4	Q	X	S	D	L	V	u	t	b	i	o	p	2
4	n	x	p	o	c	g	B	S	A	F	T	R	1
3	h	l	d	y	u	m	J	K	E	Q	V	I	2
2	v	e	k	i	j	q	U	D	L	M	H	Y	3
1	t	a	s	r	b	f	C	P	X	G	N	O	4
	5	3	2	6	1	4	1	2	3	4	5	6	

Z	1	2	3	4	3	4	1	2	
1	A	O	F	Q	r	l	n	u	5
2	J	B	M	X	c	s	g	t	3
3	G	T	C	S	m	x	j	b	2
4	K	P	H	D	y	v	e	i	6
5	N	U	R	L	f	q	a	o	1
6	E	I	Y	V	h	d	k	p	4
4	m	g	f	q	B	J	U	C	1
5	h	n	t	v	S	K	D	P	2
6	y	o	r	i	A	E	L	X	3
1	u	c	b	j	F	Q	M	G	4
2	d	p	s	k	T	V	H	N	5
3	l	x	a	e	R	I	Y	O	6
	3	4	1	2	1	2	3	4	

Les conditions assurant la réciprocité sont les mêmes que pour les carrés; ces conditions étant remplies, chacun des deux damiers ci-dessus jouit de la réciprocité.

On remarquera que, bien que formés des mêmes alphabets principaux semblablement ordonnés, ces deux damiers ne fournissent qu'un fort petit nombre de bigrammes identiques.

Nous pouvons aussi former des demi-damiers rectangulaires, tant horizontaux que verticaux.

Demi-damiers verticaux.

Z N° 1.

C	G	M	T
V	S	D	K
H	Y	P	N
E	X	R	I
L	B	F	A
U	O	J	Q
D	C	O	M
Y	H	Q	E
K	U	T	V
S	I	F	N
P	L	A	X
R	G	J	B

Z N° 2.

C	V	H	E	L	U
G	S	Y	X	B	O
M	D	P	R	F	J
T	K	N	I	A	Q
D	Y	K	S	P	R
C	H	U	I	L	G
O	Q	T	F	A	J
M	E	V	N	X	B

Demi-damiers horizontaux.

Z N° 3.

C	V	H	E	L	U	D	Y	K	S	P	R
G	S	Y	X	B	O	C	H	U	I	L	G
M	D	P	R	F	J	O	Q	T	F	A	J
T	K	N	I	A	Q	M	E	V	N	X	B

Z N° 4.

C	G	M	T	D	C	O	M
V	S	D	K	Y	H	Q	E
H	Y	P	N	K	U	T	V
E	X	R	I	S	I	F	N
L	B	F	A	P	L	A	X
U	O	J	Q	R	G	J	B

Nous devons faire ici deux remarques importantes, qui s'appliquent à tous les demi-damiers, qu'ils soient constitués par des rectangles ou par des carrés :

La première, c'est que les demi-damiers verticaux jouissent toujours de la réciprocité ;

La seconde c'est que, si on emploie un même demi-damier verticalement et horizontalement, on obtient un bigramme formé des mêmes chiffres changés de place. Tel est le cas pour les demi-damiers numéros 1 et 3 et pour ceux numéros 2 et 4.

Exemple :	*vi*	*ve*	*la*	*Fr*	*an*	*ce*
N° 1	SS	KY	FP	LJ	AN	TY
N° 3	SS	YK	PF	JL	NA	YT
N° 2	EH	VE	LA	JP	IX	VM
N° 4	HE	EV	AL	PJ	XI	MV

Enfin, de même que les carrés, les rectangles alphabétiques simples peuvent servir à bigraphier :

K N° 1.

A	J	G	L	O	E
P	B	U	Q	V	I
F	N	C	H	S	Z
R	Y	T	D	M	X

K N° 2.

A	P	F	R
J	B	N	Y
G	U	C	T
L	Q	H	D
O	V	S	M
E	I	Z	X

Il est bon de faire remarquer que le rectangle disposé horizontalement, comme l'indique la figure numéro 1, présente plus de garanties de secret que celui de la figure numéro 2. Dans le premier, sur les cinq cent soixante-seize bigrammes, quatre-vingt-seize sont chiffrés par eux-mêmes, tandis que, dans le second, il y en a cent quarante-quatre. Ce petit défaut n'entrainera, du reste, aucun inconvénient lorsqu'on fera usage de bigrammes *rompus* ou de bigrammes *scindés*.

La même observation s'applique aux demi-damiers ; le nombre des bigrammes chiffrés par eux-mêmes, ou non chiffrés, s'élève à quatre-vingt-seize sur cinq cent soixante-seize pour les demi-damiers horizontaux, et à cent quarante-quatre sur cinq cent soixante-seize pour les demi-damiers verticaux. Ces nombres sont inverses pour les bigrammes retournés ou renversés.

Alphabets bifides ou à deux chiffres. — On peut encore bigraphier au moyen d'alphabets permettant de rompre chaque lettre en deux fragments qui, joints aux fragments d'autres lettres, produisent les deux chiffres du bigramme cryptographique.

Pour former les alphabets bifides, nous attribuerons à chaque lettre un groupe de deux signes ; les signes les plus simples étant les chiffres arabes, c'est de ceux-ci que nous ferons usage.

Chaque lettre sera donc représentée par un nombre de deux chiffres. Mais, s'il est indispensable qu'à chaque lettre corresponde un groupe différent, c'est-à-dire qu'il y ait autant de combinaisons de chiffres qu'il y a de lettres, il est tout aussi indispensable qu'il y ait autant de lettres que de groupes numériques. S'il en était autrement, une combinaison de chiffres produite par la fragmentation des groupes pourrait ne pas se trouver représentée et le chiffrage deviendrait impossible.

Cette nécessité inéluctable fixe à *cinq* le nombre des chiffres à employer. En effet, le total des combinaisons que l'on peut former avec cinq objets groupés deux à deux, de toutes les manières possibles est de $5 \times 5 = 25$, nombre des lettres de l'alphabet.

Venons à l'application et formons d'abord un alphabet. Pour plus de simplicité, prenons l'alphabet bifide normal, en laissant les lettres et les groupes numériques dans leur ordre naturel, pour que l'alphabet soit, à la fois, *chiffrant* et *déchiffrant* :

A = 11	F = 21	K = 31	P = 41	U = 51
B = 12	G = 22	L = 32	Q = 42	V = 52
C = 13	H = 23	M = 33	R = 43	X = 53
D = 14	I = 24	N = 34	S = 44	Y = 54
E = 15	J = 25	O = 35	T = 45	Z = 55

Pour bien saisir le mécanisme du chiffrement, prenons quelques-uns des groupes numériques du tableau ci-dessus ; superposons-les deux à deux, puis, les lisant verticalement et horizontalement, cherchons leurs valeurs littérales, nous aurons :

C I	J K	L Y	B N	H U	O I
‖ ‖	‖ ‖	‖ ‖	‖ ‖	‖ ‖	‖ ‖
1 2 = B	2 3 = H	3 5 = O	1 3 = C	2 5 = J	3 2 = L
3 4 = N	5 1 = U	2 4 = I	2 4 = I	3 1 = K	5 4 = Y

Nous voyons que, selon le mode de lecture des groupes numériques : CI = *bn*, JK = *hu*, LY = *oi* et que réciproquement : BN = *ci*, HU = *jk* et OI = *ly*.

Ceci suffit pour prouver que les alphabets bifides peuvent servir à la formation des tableaux de bigrammes réciproques ou, plus pratiquement les remplacer, de même que les damiers bigrammatiques, et fournir exactement les mêmes résultats que ces derniers dans beaucoup de cas, surtout lorsque l'on fait usage de bigrammes fixes, entiers ou rompus, en chiffrant les lettres claires sans transposition.

Alphabets bifides intervertis. — Pour intervertir un alphabet bifide, il suffit d'intervertir la série littérale ou la série numérique, en laissant l'autre dans l'ordre normal.

Soit l'alphabet interverti :

Alphabet Chiffrant		*Alphabet Déchiffrant*	
A = 42	N = 12	11 = G	34 = E
B = 22	O = 55	12 = N	35 = T
C = 14	P = 33	13 = U	41 = J
D = 32	Q = 31	14 = C	42 = A
E = 34	R = 52	15 = K	43 = Y
F = 25	S = 21	21 = S	44 = X
G = 11	T = 35	22 = B	45 = Z
H = 53	U = 13	23 = L	51 = I
I = 51	V = 24	24 = V	52 = R
J = 41	X = 44	25 = F	53 = H
K = 15	Y = 43	31 = Q	54 = M
L = 23	Z = 45	32 = D	55 = O
M = 54		33 = P	

Les alphabets chiffrant et déchiffrant ne diffèrent l'un de l'autre qu'en ce que, dans l'alphabet chiffrant, les lettres sont dans l'ordre normal, tandis que dans le déchiffrant, ce sont les groupes numériques qui sont classés dans l'ordre naturel ; mais la valeur des lettres est la même dans les deux alphabets.

Soit à bigraphier :

On a souvent besoin d'un plus petit que soi.

Pour cela, ayant écrit le texte clair en espaçant un peu les lettres et les groupant deux à deux, nous inscrirons *verticalement* sous chacune d'elles le nombre qui lui correspond ; ensuite, relevant *horizontalement* ces nombres, d'abord celui de la ligne supérieure de chaque groupe, puis celui de la ligne inférieure, nous en cherchons la valeur littérale dans l'alphabet déchiffrant

et les bigrammes ainsi trouvés formeront le cryptogramme demandé :

on	*as*	*ou*	*ve*	*nt*	*be*	*so*	*in*	*du*	*np*	*lu*	*sp*	*et*	*it*	*qu*	*es*	*oi*
51	42	51	23	13	23	25	51	31	13	21	23	33	53	31	32	55
52	21	53	44	25	24	15	12	23	23	33	13	45	15	13	41	51
IR	AS	IH	LX	UF	LV	FK	IN	QL	UL	SP	LU	PZ	HK	QU	DJ	OI

Avec le demi-damier vertical ci-après, on aurait obtenu le même cryptogramme, savoir :

IRASIHLXUFLVFKINQLULSPLUPZHKQUDJOI

G	N	U	C	K
S	B	L	V	F
Q	D	P	E	T
J	A	Y	X	Z
I	R	H	M	O
G	S	Q	J	I
N	B	D	A	R
U	L	P	Y	H
C	V	E	X	M
K	F	T	Z	O

Nous avons vu que les damiers bigrammatiques permettent de chiffrer simultanément deux lignes claires.

On pourrait obtenir le même résultat avec un alphabet bifide ; il faudrait, pour cela, écrire le texte sur deux lignes en espaçant les lettres suffisamment afin d'inscrire leurs valeurs numériques au-dessous et *horizontalement*, de préférence ; transformer ensuite les nombres lus *verticalement* en lettres que l'on écrira, suivant les conventions, sur une, ou sur deux lignes, dont le relèvement se fera selon le mode convenu :

o	*n*	*a*	*s*	*o*	*u*	*v*	*e*	*n*	*t*	*b*	*e*	*s*	*o*	*i*	*n*	*d*
u	*n*	*p*	*l*	*u*	*s*	*p*	*e*	*t*	*i*	*t*	*q*	*u*	*e*	*s*	*o*	*i*
55	12	42	21	55	13	24	34	12	35	22	34	21	55	51	12	32
13	12	33	23	13	21	33	34	35	51	35	31	13	34	21	55	51
I	G	Y	B	I	N	L	P	U	T	L	P	S	H	R	K	T
H	B	L	U	H	Q	Y	X	F	I	F	J	U	M	G	F	S

Le demi-damier ci-dessus fournit le même cryptogramme, ainsi qu'il est facile de s'en assurer.

Avec les alphabets bifides, la traduction se fait comme le chiffrement, en écrivant ou lisant *horizontalement* les chiffres écrits ou lus *verticalement* dans la première opération et *vice versa.*

Alphabets bifides conjugués. — Afin d'augmenter les garanties de secret, on peut faire usage, en même temps, de deux alphabets bifides. Le premier sert alors à transformer les lettres claires en chiffres et le second est utilisé pour convertir ces chiffres, lus comme dans le cas d'un simple alphabet, en de nouvelles lettres formant le cryptogramme.

Soient deux alphabets bifides, dont nous ne donnons que le tableau chiffrant de l'un et le déchiffrant de l'autre, ce qui suffit pour le chiffrement; pour la traduction, les alphabets inverses seraient plus commodes :

N° 1. *Chiffrant.*		N° 2. *Déchiffrant.*	
A = 12	N = 14	11 = J	34 = T
B = 22	O = 34	12 = Z	35 = Q
C = 41	P = 54	13 = V	41 = I
D = 35	Q = 32	14 = G	42 = D
E = 21	R = 53	15 = R	43 = E
F = 45	S = 33	21 = A	44 = C
G = 31	T = 13	22 = U	45 = S
H = 11	U = 43	23 = H	51 = Y
I = 24	V = 23	24 = F	52 = N
J = 42	X = 15	25 = M	53 = L
K = 55	Y = 52	31 = O	54 = X
L = 25	Z = 51	32 = K	55 = P
M = 44		33 = B	

Pour bigraphier, il faut écrire *verticalement* sous chaque lettre sa valeur numérique prise dans l'alphabet n° 1, puis relever les chiffres *horizontalement* et les transformer en lettres à l'aide de l'alphabet numéro 2.

Pour exemple, bigraphions la dépêche suivante :

Situation très critique. Besoin urgent de renfort.

si	*tu*	*at*	*io*	*nt*	*re*	*sc*	*ri*	*ti*	*qu*	*eb*	*es*	*oi*	*nu*	*rg*	*en*	*td*	*er*	*en*	*fo*	*rt*
32	14	11	23	11	52	34	52	12	34	22	23	32	14	53	21	13	25	21	43	51
34	33	23	44	43	31	31	34	34	23	12	13	44	43	31	14	35	13	14	54	33
K	G	J	H	J	N	T	N	Z	T	U	H	K	G	L	A	V	M	A	E	Y
T	B	H	C	E	O	O	T	T	H	Z	V	C	E	O	G	Q	V	G	X	B

Le damier bigrammatique ci-dessous aurait fourni le même cryptogramme :

	H	A	T	N	X	j	z	v	g	r	
	E	B	V	I	L	a	u	h	f	m	
1	G	Q	S	O	D	o	k	b	t	q	2
	C	J	U	M	F	i	d	e	c	s	
	Z	Y	R	P	K	y	n	l	x	p	
	j	a	o	i	y	H	E	G	C	Z	
	z	u	k	d	n	A	B	Q	J	Y	
4	v	h	b	e	l	T	V	S	U	R	3
	g	f	t	c	x	N	I	O	M	P	
	r	m	q	s	p	X	L	D	F	K	

On aurait encore pu arriver au même résultat en bigraphiant avec l'alphabet numéro 1 seul et en chiffrant le cryptogramme obtenu à l'aide de l'alphabet suivant, d'après la méthode monoalphabétique :

A B C D E F G H I J K L M N O P Q R S T U V X Y Z
z u i q a s o j f d p m c g t x k l b v e h r n y

La traduction se fait par l'opération inverse du chiffrement ; seulement, si on fait usage du damier, il ne faut pas oublier que, la réciprocité n'existant pas, les carrés 1 et 3, écrits en capitales, sont uniquement applicables aux lettres claires ; les lettres du cryptogramme doivent donc être cherchées dans les deux autres carrés.

Alphabets bifides incomplets ou mélangés. — Cette longue comparaison des alphabets bifides et des damiers bigrammatiques a surtout pour objet de montrer que ces derniers opèrent réellement la fragmentation des lettres et de permettre d'en suivre les fragments dans toutes les combinaisons. Il semble donc indispensable, au point de vue théorique, d'examiner comment les damiers *rectangulaires* peuvent se rattacher aux alphabets bifides, la loi fondamentale de ces derniers étant violée, puisque le nombre des lettres n'est pas égal à celui des combinaisons numériques possibles.

Afin de mieux suivre les fractions de lettres, au lieu de les représenter par deux chiffres, nous ferons usage d'un chiffre et d'une petite lettre ; la position de ces éléments variera dans

chacun des alphabets employés simultanément : si la lettre précède le chiffre dans l'un, dans l'autre, elle devra le suivre.

Formons deux alphabets réduits à six lettres et le damier rectangulaire correspondant :

Alphabet N° 1.

A = 1 a	D = 2 a
B = 1 b	E = 2 b
C = 1 c	F = 2 c

Alphabet N° 2.

A = b 1	D = c 1
B = c 2	E = b 2
C = a 2	F = a 1

A	B	C
D	E	F
F	A	D
C	E	B

On bigraphie en inscrivant *verticalement* sous chaque lettre sa valeur numérique prise dans l'alphabet numéro 1 pour les *premières* lettres de chaque groupe et dans l'alphabet numéro 2 pour les *secondes ;* on convertit ensuite les chiffres en lettres, le premier groupe *horizontal* appartenant à l'alphabet numéro 1, et le deuxième à l'alphabet numéro 2, comme, du reste, l'indique la composition des groupes numériques.

Exemple :	C E	D A	C A	F E
	‖ ‖	‖ ‖	‖ ‖	‖ ‖
	1 *b* = B	2 *b* = E	1 *b* = B	2 *b* = E
	c 2 = B	*a* 1 = F	*c* 1 = D	*c* 2 = B

D'après le damier, on aurait : *céda* = BBEF, *café* = BDEB.

Ceci semblant suffisant pour guider les études des lecteurs désireux de se rendre compte des transformations bigrammatiques, nous allons rechercher les moyens d'augmenter les garanties de secret avec chacune des méthodes étudiées ci-dessus.

Les bigrammes *fixes* pouvant offrir quelques indices au déchiffreur ennemi, nous avons indiqué le moyen de les fractionner et de transposer, en même temps, les dépêches. Ces procédés semblent offrir toute sécurité, mais il est préférable et plus sûr encore de faire usage des bigrammes *variables* ou *scindés*.

Bigrammes variables. — Nous avons vu que chaque lettre pouvant être représentée par deux chiffres, les quatre fragments de lettres formant un bigramme *clair* donnent, par leur permutation, un bigramme *secret*. Dans les méthodes qui suivent, les deux fragments de chaque lettre sont séparés : le premier s'associe à l'un des fragments d'une lettre voisine et le deuxième à l'un des fragments d'une *autre* lettre.

Désormais, nous ne ferons plus le rapprochement entre les alphabets bifides et les damiers bigrammatiques ; chacun de ces systèmes ayant son caractère spécial, le résultat facilement fourni par l'un d'eux ne pourrait être obtenu de l'autre sans complications, qu'il importe toujours d'éviter.

Scission des bigrammes par alphabets bifides. — Comme précédemment, nous écrirons *verticalement*, sous chaque lettre du texte clair, sa valeur numérique ; nous séparerons ensuite ces lettres en groupes, réguliers ou non, selon les conventions arrêtées avec notre correspondant, mais *toujours d'un nombre impair de lettres*, les nombres *pairs* ne pouvant fournir que des bigrammes *fixes*, quoique rompus ; enfin la conversion des chiffres en lettres nouvelles se fait, comme précédemment, par la lecture *horizontale* des chiffres, le dernier de la première ligne s'associant au premier de la deuxième pour former un groupe.

Dans l'exemple ci-dessous, afin de mettre bien en évidence le mouvement des fragments de lettres et les combinaisons qu'ils forment, nous remplacerons les chiffres, représentant ces fragments, par la lettre claire accompagnée d'un indice faisant connaitre la place occupée par ces fragments, les différenciant en un mot ; nous ferons donc : $A = a_1 a_2$, $T = t_1 t_2$, $E = e_1 e_2$, $N = n_1 n_2$, etc.

A T T E N	D E Z	D E S O R	D R E	S
a_1 t_1 t_1 e_1 n_1	d_1 e_1 z_1	d_1 e_1 s_1 o_1 r_1	d_1 r_1 e_1	s_1
a_2 t_2 t_2 e_2 n_2	d_2 e_2 z_2	d_2 e_2 s_2 o_2 r_2	d_2 r_2 e_2	s_2

Divisons notre dépêche par groupes alternés de cinq et trois lettres. Le dernier groupe, ne contenant qu'une lettre, sera chiffré par lui-même.

La première lettre du cryptogramme sera déterminée par $a_1 t_1$, la deuxième par $t_1 e_1$, la troisième par $n_1 a_2$, la quatrième par $t_2 t_2$ et la cinquième par $e_2 n_2$. Le deuxième groupe donnera les valeurs : $d_1 e_1$, $z_1 d_2$ et $e_2 z_2$ pour les lettres du chiffre.....

On voit clairement qu'après cette opération les lettres primitives n'existent plus et que leurs fragments, ou éléments constitutifs, sont dispersés au hasard des groupements adoptés. Ainsi, dans le deuxième groupe D E Z, le premier fragment de D s'associe avec le premier de E, le premier de Z avec le deuxième de D et enfin le deuxième de E avec le deuxième de Z.

Maintenant chiffrons, avec l'alphabet de la page 87, la même dépêche divisée en groupes de *cinq* lettres. Le dernier groupe, n'en contenant que *deux*, donnera un bigramme *fixe*.

a t t e n	*d e z d e*	*s o r d r*	*e s*
4 3.3 3.1	3 3.4 3.3	2 5.5 3.5	3 2.
2.5 5.4 2	2.4 5.2 4.	1.5 2.2 2.	4 1.
Y P N O A	P Y D Z V	F H I R B	D J

43 = Y, 33 = P, 12 = N, 55 = O, 42 = A, etc.

Autre exemple : Groupons par *sept* et chiffrons avec les alphabets conjugués de la page 89 ; il viendra :

a t t e n d e	*z d e s o r d*	*r e s*
1 1.1 2.1 3.2	5 3.2 3.3 5.3	5 2.3
2.3 3.1 4.5 1.	1 5 1.3 4.3 5.	3.1 3.
J Z V U B G Y	L H Q O Y T Q	N B V

Si nous avions converti nos chiffres en lettres avec l'alphabet numéro 1, qui a servi à fragmenter les *claires*, nous aurions obtenu le cryptogramme suivant :

HATBSNZ RVDGZOD YST

qui, chiffré à son tour avec l'alphabet monolittéral de la page 90, reproduit le premier cryptogramme.

La traduction est, comme toujours, l'inverse du chiffrement et ne présente aucune difficulté.

Nous ne pouvons examiner toutes les combinaisons que l'on peut obtenir avec les alphabets bifides, mais il semble indispensable de signaler celles qu'on obtient à l'aide des *tours de clé multiples*, ces combinaisons permettant une facile transposition des fragments de lettres et même un second chiffrement monolittéral des cryptogrammes.

Tours de clé multiples. — Après avoir écrit *verticalement*, sous les lettres claires, les groupes numériques qui leur correspondent, au lieu de les convertir immédiatement en lettres, après les avoir relevés *horizontalement*, on les écrit *verticalement* au-dessous des premiers, de manière à former un nouveau tableau, que l'on relève *horizontalement* et transforme en lettres cryptographiques.

Pour bien montrer la disjonction des éléments de chaque lettre et la constitution des chiffres du cryptogramme, nous allons appliquer la méthode aux premières lettres de l'alphabet normal, prises comme texte clair, que nous grouperons une première fois par trois et une seconde par neuf. Les moitiés de chaque lettre seront, comme précédemment, représentées par la lettre elle-même accompagnée d'un indice : A = a_1 a_2, B = b_1 b_2, C = c_1 c_2,... etc.

A B C	D E F	G H I
a_1 b_1 c_1	d_1 e_1 f_1	g_1 h_1 i_1
a_2 b_2 c_2	d_2 e_2 f_2	g_2 h_2 i_2

a_1 c_1' b_2 d_1' f_1 e_2' g_1 i_1' h_2
b_1' a_2 c_2' e_1 d_2' f_2 h_1' g_2 i_2

Un nouveau relevé horizontal fixera la composition des lettres du cryptogramme, dont la valeur sera :

$a_1 c_1 - b_2 d_1 - f_1 e_2 - g_1 i_1 - h_2 b_1 - a_2 c_2 - e_1 d_2 - f_2 h_1 - g_2 i_2$.

On voit clairement que les moitiés de lettres claires sont absolument disjointes et qu'aucune d'elles ne s'associe avec les fragments des lettres voisines et on conçoit que leur transposition est entièrement masquée après la conversion des *bigrammes fragmentaires* en lettres simples.

Les groupements sont absolument arbitraires ; il en est de même du nombre des relevés et transcriptions intermédiaires, pourvu que ces opérations soient fixées par les conventions.

On peut aussi employer deux alphabets conjugués, le premier servant à la décomposition des claires et le second à la détermination des lettres du cryptogramme, ce qui, comme nous l'avons déjà vu, revient à chiffrer à l'aide d'un alphabet monolittéral le cryptogramme fourni par un alphabet bifide unique.

La traduction s'obtient par l'opération inverse de celle qui a servi au chiffrement.

Scission des bigrammes par damiers, demi-damiers et carrés ou rectangles alphabétiques. — Pour bien nous rendre compte du mouvement des demi-lettres dans cette nouvelle méthode et de la différence qui existe entre elle et la méthode précédente, formons un damier bigrammatique complet avec les groupes numériques de l'alphabet bifide normal :

	11	12	13	14	15	11	12	13	14	15	
	21	22	23	24	25	21	22	23	24	25	
1	31	32	33	34	35	31	32	33	34	35	2
	41	42	43	44	45	41	42	43	44	45	
	51	52	53	54	55	51	52	53	54	55	
	11	21	31	41	51	11	21	31	41	51	
	12	22	32	42	52	12	22	32	42	52	
4	13	23	33	43	53	13	23	33	43	53	3
	14	24	34	44	54	14	24	34	44	54	
	15	25	35	45	55	15	25	35	45	55	

Tel est le damier numérique *fondamental ;* les chiffres n'en peuvent varier. Comme nous l'avons dit, les quartiers 1 et 3 renferment les alphabets principaux, exclusivement consacrés aux lettres claires, tandis que les quartiers 2 et 4 contiennent les alphabets auxiliaires, uniquement consacrés aux lettres secrètes.

Le quartier numéro 2 fournit la première lettre du bigramme cryptographique; ses groupes numériques sont constitués par le chiffre des dizaines de la première lettre claire, prise dans le quartier numéro 1, suivi du chiffre des dizaines de la seconde claire, prise dans le quartier numéro 3. Les chiffres des unités des deux claires forment le groupe numérique de la seconde lettre du bigramme secret, donné par le quatrième quartier. Dans les deux cas, les chiffres appartenant à la première lettre claire sont employés pour les dizaines et ceux de la seconde claire pour les unités, ainsi : 12.34 donnent 13.24 et 34.12 fournissent 31.42.

En substituant, dans chaque carré, les lettres ABC... FG... aux groupes 11, 12, 13,... 21, 22,... les bigrammes fournis par le damier sont identiques à ceux que donne l'alphabet bifide normal. De même, chaque fois que les mêmes groupes numériques représentent les mêmes lettres dans les quatre carrés du damier, les bigrammes obtenus peuvent être fournis par un alphabet bifide unique.

Dans ce cas, les carrés 2 et 4 du damier étant respectivement semblables aux carrés 1 et 3, les carrés auxiliaires 2 et 4 peuvent être supprimés, le demi-damier vertical fournissant les mêmes bigrammes secrets que le damier complet.

Lorsque les mêmes groupes numériques sont attribués à des lettres différentes dans les quatre carrés, *quatre* alphabets bifides sont nécessaires pour obtenir le résultat fourni par le damier. Au lieu de quatre alphabets, on peut cependant n'en employer qu'un seul, à condition de chiffrer avec *trois* alphabets monolittéraux, d'abord la moitié des bigrammes clairs, à l'aide du premier, puis la première lettre des bigrammes secrets, avec le deuxième et, enfin, la deuxième lettre des bigrammes secrets, avec le troisième :

Groupes numériq.	1	2	3	4	Groupes numériq.	1	2	3	4
11	Q	f	R	g	34	L	q	X	r
12	H	s	K	v	35	S	z	T	f
13	K	b	F	s	41	U	c	M	p
14	Z	p	N	m	42	R	g	V	q
15	E	l	D	c	43	C	r	C	u
21	A	m	H	x	44	J	u	G	o
22	Y	v	B	a	45	G	j	S	y
23	T	o	I	t	51	X	t	O	l
24	N	x	L	e	52	O	i	Q	b
25	I	d	J	z	53	M	y	Y	j
31	P	k	E	n	54	D	a	P	h
32	B	e	A	k	55	V	n	U	i
33	F	h	Z	d					

Pour cryptographier le mot : *République*, en bigrammes entiers, après l'avoir divisé en groupes de deux lettres, nous substituons à la seconde de chaque groupe, prise dans l'alphabet 3, celle qui lui correspond dans l'alphabet 1, afin de pouvoir appliquer le même alphabet bifide, puis nous chiffrons :

Re pu bl iq ue — e=p, u=v, l=n, q=o, e=p,

d'où

	Rp	*pv*	*bn*	*io*	*up*
	43	35	32	25	43
	21	15	24	52	11
	C	S	B	I	C
	A	E	N	O	Q

Les lettres secrètes appartenant à l'alphabet numéro 1, il reste à les traduire en deux et quatre, en substituant aux lettres de la première ligne celles qui leur correspondent dans l'alphabet numéro 2, et à celles de la seconde ligne leurs correspondantes de l'alphabet numéro 4 ; il vient finalement :

Re	*pu*	*bl*	*iq*	*ue*
RX	ZC	EE	DB	RG

résultat qu'une *seule* opération nous aurait fourni en employant le tableau de la page 74, ou le damier de la page 77.

Quand on se donne la peine de former le tableau des références ci-dessus, on peut, au lieu de chiffrer les lettres avec des alphabets monolittéraux, faire usage des groupes numériques en les appliquant successivement à chaque alphabet, mais nombreuses sont les chances d'erreur.

Lorsque les carrés 2 et 4 du damier sont respectivement semblables aux carrés 3 et 1, le demi-damier horizontal donne les mêmes résultats que le damier complet. Dans ce cas, les lettres secrètes ont pour groupes numériques ceux des lettres claires modifiés par l'échange du chiffre des unités :

12.34 = 14.32, 34.12 = 32.14

Le même résultat est obtenu quand les deux alphabets d'un demi-damier, horizontal ou vertical, étant identiquement semblables, le damier se réduit à un carré alphabétique.

Les observations qui précèdent, jointes aux indications déjà données, nous dispensent d'étudier spécialement les damiers rectangulaires complets ou réduits. Il sera facile au lecteur, que cette étude intéresse, de se rendre un compte exact du mouvement des fragments de lettres.

Ceci posé, on obtient la *scission des bigrammes* de la manière suivante :

Damiers complets, carrés ou rectangulaires.

Prendre pour première lettre du cryptogramme la lettre qui, dans le deuxième quartier, se trouve à l'intersection de la rangée occupée par la première lettre claire et de la colonne où se trouve la deuxième claire.

Prendre pour deuxième lettre du cryptogramme celle qui, dans le quatrième quartier, se trouve à l'intersection de la rangée occupée par la deuxième claire et de la colonne où se trouve la troisième claire.

Continuer ainsi, en formant une sorte d'hélice, chaque lettre secrète étant déterminée dans les alphabets auxiliaires 2 et 4, par la rencontre de la rangée de la première lettre considérée et de la colonne de la seconde.

Le diagramme suivant montre comment les deux fragments de chaque lettre claire s'associent aux fragments des lettres voisines. Pour plus de clarté, nous prendrons comme texte clair les premières lettres de l'alphabet normal, en faisant : $A = a_1\ a_2$, $B = b_1\ b_2$, $C = c_1\ c_2 \ldots$, etc., et en désignant par une flèche l'ordre de combinaison des fragments, ainsi : $a_1 \longrightarrow b_1$ indique le chiffre $a_1\ b_1$ ayant a_1 pour premier fragment et b_1 pour second, tandis que $a_1 \longleftarrow b_1$ donnera le chiffre $b_1\ a_1$, dont les fragments sont invertis.

Lettres claires :

H	A	B	C	D	E	F	G	H	A
$h_1 \longrightarrow$	a_1	$b_1 \longrightarrow$	c_1	$d_1 \longrightarrow$	e_1	$f_1 \longrightarrow$	g_1	$h_1 \longrightarrow$	a_1
	$a_2 \longleftarrow$	b_2	$c_2 \longleftarrow$	d_2	$e_2 \longleftarrow$	f_2	$g_2 \longleftarrow$	h_2	

Lettres chiffres :

h_1a_1	b_2a_2	b_1c_1	d_2c_2	d_1e_1	f_2e_2	f_1g_1	h_2g_2	h_1a_1
R	S	T	U	V	X	Y	Z	R

On voit qu'à proprement parler il n'existe plus de bigrammes et que chaque lettre doit se décomposer pour se combiner avec ses deux voisines de manière à former deux lettres du cryptogramme. Il en résulte que la première et la dernière lettres ne sont pas spécifiées. Pour obvier à cet inconvénient, il suffit, si le nombre de lettres à chiffrer est *pair*, de faire précéder le texte clair de la dernière lettre du texte entier, ou d'un groupe convenu, et de chiffrer, en outre, cette lettre à la fin du texte, ou du groupe, de manière à obtenir autant de lettres chiffres qu'il y a de lettres claires. Mais, si le nombre des lettres à cryptographier est *impair*, le dernier chiffre n'étant pas le même que le premier, le cryptogramme doit avoir une lettre de plus que le texte clair, ce qu'on obtient en reportant à la fin la première lettre du texte, comme nous l'avons fait ci-dessus.

Cette règle s'applique à tous les damiers complets ou incomplets, carrés ou rectangulaires ; la seule exception qu'elle puisse comporter, pour un nombre de lettres impair, s'applique aux carrés et rectangles alphabétiques et provient de ce que la lettre reportée est prise, au commencement et à la fin, dans le même alphabet, tandis que, dans les autres cas, elle est prise successivement dans deux alphabets et, par suite, se traduit par deux chiffres différents. Cependant, pour la facilité de la traduction, il vaut mieux ne pas profiter de cette simplification.

Dans les *demi-damiers verticaux*, les éléments des lettres se combinent comme dans les damiers complets, tandis que, dans les *demi-damiers horizontaux* et dans les *carrés ou rectangles alphabétiques*, leur mouvement est différent, bien que le mode de chiffrage reste le même.

Le diagramme ci-après indique ce mouvement :

Lettres claires	E	A	B	C	D	E	A
	e_1 ↘	a_1 ↘	b_1 ↘	c_1 ↘	d_1 ↘	e_1 ↘	a_1
	e_2	a_2	b_2	c_2	d_2	e_2	a_2
Lettres-chiffres		e_1a_2	a_1b_2	b_1c_2	c_1d_2	d_1e_2	e_1a_2
		T	U	V	X	Y	Z

Appliquons la méthode à quelques exemples : la dernière lettre est reportée en tête du texte clair, et la première est répétée à la fin :

1° Damier complet de la page 77

e... I l f a u t a u t a n t q u'o n p e u t...
S U K S D F O V R C M R D V J P D H L F

t o b l i g e r t o u t l e m o n d e... i
D X E H X H F N D G R Y H N N P M I S

2° Demi-damier horizontal de la page 80

s... P a t i e n c e e t l o n g u e u r
M U T D E I G T H J F J O B V T T R F

d e t e m p s... p
O T E N P U K

3° Carré alphabétique de la page 82

e... F o n t p l u s q u e f o r c e
L P O Y M F E S S Y U L P D R T

n i q u e r a g e... f
V H K Y U R A L U L

La traduction n'offre pas de difficulté; c'est toujours l'opération inverse du chiffrement. Il convient cependant de faire remarquer que la réciprocité n'existant, dans le cas actuel, pour aucun des damiers, les lettres-chiffres doivent toujours être cherchées dans les alphabets auxiliaires, deux et quatre, des damiers complets, les alphabets principaux étant exclusivement réservés aux lettres claires, sauf conventions contraires bien entendu.

Dans les damiers incomplets, c'est-à-dire les demi-damiers et les carrés ou rectangles alphabétiques, le chiffrement se faisant normalement en prenant la *lettre-chiffre dans la colonne de la deuxième claire*, il faudra, pour la traduction, prendre la *claire dans la colonne de la première lettre-chiffre*.

Soit à traduire le cryptogramme suivant, qui a été chiffré avec le carré alphabétique normal :

A	B	C	D	E
F	G	H	I	J
K	L	M	N	O
P	Q	R	S	T
U	V	X	Y	Z

D E A X Y P X T E T D Q U B O D O R
d e u x s û r e t é s v a l e n t

N J A X V P U Y O D
m i e u x q u' u n e

Nous avons vu comment les fragments des lettres claires se dissocient et se combinent pour former les lettres chiffres, dissociation et combinaison mises en évidence par le diagramme :

Lettres claires :

E	D	E	U	X	S	U	R	E	T	E	S	V	A
e_1	d_1	e_1	u_1	x_1	s_1	u_1	r_1	e_1	t_1	e_1	s^1	v_1	a_1
e^2	d^2	e_2	u_2	x_2	s_2	u_2	r_2	e_2	t_2	e_2	s_2	v_2	a_2

Lettres chiffres :

e_1d_2	d_1e_2	e_1u_2	u_1x_2	x_1s_2	s_1u_2	u_1r_2	r_1e_2	e_1t_2	t_1e_2	e_1s_2	s_1v_2	v_1a_2	a_1
D	E	A	X	Y	P	X	T	E	T	D	Q	U	B

Le diagramme ci-après montre la reconstitution des lettres claires par la dissociation et la combinaison des éléments constitutifs des lettres chiffres :

Lettres chiffres :

D	E	A	X	Y	P	X	T	E	T	D	Q	U	B
e_2	d_1	e_1	u_1	x_1	s_1	u_1	r_1	e_1	t_1	e_1	s_1	v_1	a_1
d_2	e_2	u_2	x_2	s_2	u_2	r_2	e_2	t_2	e_2	s_2	v_2	a_2	.

Lettres claires :

d_1d_2	e_1e_2	u_1u_2	x_1x_2	s_1s_2	u_1u_2	r_1r_2	e_1e_2	t_1t_2	e_1e_2	s_1s_2	v_1v_2	a_1a_2
D	E	U	X	S	U	R	E	T	E	S	V	A

On voit qu'il ne peut se produire aucune ambiguïté pour peu qu'on applique le procédé avec la précision nécessaire, précision qu'on obtiendra facilement avec un peu d'exercice

Remarque importante. — Ce qui trouble le plus les personnes peu familiarisées avec cette méthode, c'est la nécessité de lire, pour la traduction, la lettre cherchée dans la *colonne de la première lettre chiffre*, tandis que, dans le chiffrement, on la lit dans la *colonne de la deuxième claire*. Cet inconvénient peut être facilement évité, en *commençant la traduction* par la *dernière* lettre chiffre et en remontant vers la première. Le chiffrement et la traduction se font alors d'une façon identique, en lisant la lettre cherchée dans la colonne de la deuxième lettre à traduire et la rangée de la première.

Le cryptogramme ci-dessus se traduira donc ainsi :

..... U B O D O R N J A X V P U Y O D.
a l e n t m i e u x q u u n e.

DO détermine *e*, OY—*n*, YU—*u*, UP—*u*, PV—*q*....

Cette méthode, très pratique pour les damiers réduits à un ou à deux carrés ou rectangles alphabétiques, ne présente pas d'avantages pour les damiers complets, dont la lecture serait simplement inversée, sans simplification aucune.

Autre remarque. — Le chiffrement par bigrammes *fixes* n'est nullement gêné par l'absence d'une lettre, omise dans la formation des rectangles. Il n'en est plus ainsi avec les bigrammes *scindés*, mais la difficulté peut être tournée, soit en donnant deux valeurs à une même lettre : K = Q, Z = S, J = I,... etc., soit en dédoublant certaines lettres : J = II, X = CS,... de sorte que toutes les lettres employées soient comprises dans le damier dont on se sert.

Observation. — Nous n'avons considéré que les damiers formés de un, deux ou quatre alphabets; les damiers de six, sept,...

alphabets donnent des résultats analogues. Nous ne croyons cependant pas devoir en entreprendre l'étude, qui allongerait notre travail, sans beaucoup d'utilité, les indications précédentes suffisant pour guider les cryptographes dans la formation et l'emploi de ces damiers.

Trigrammes.

Les alphabets *trifides*, ou à *trois chiffres*, constituent le seul moyen pratique connu de former des trigrammes cryptographiques. En effet, vingt-cinq lettres combinées trois à trois fournissent quinze mille six cent vingt-cinq groupes de ternaires ; on ne peut donc songer à rapprocher deux listes de cette longueur ; c'est à peine si on peut les disposer en tableaux ou mieux en volumes à triple entrée, dont le maniement serait certainement long et difficile.

Les alphabets trifides seuls sont d'un emploi usuel et, s'ils se prêtent difficilement à l'emploi des trigrammes *fixes*, ils fournissent facilement des trigrammes *scindés* d'une utilité et d'une sécurité indéniables.

Nous étant étendus longuement sur les alphabets bifides et sur la génération des bigrammes à l'aide de leur concours, il nous suffira d'exposer les principes des alphabets trifides et du mode de formation des trigrammes d'une manière succincte à cause de la connexité que présentent les deux systèmes.

Alphabets trifides ou à trois chiffres. — Afin de pouvoir fragmenter les lettres en trois parties, il est nécessaire de représenter chacune d'elles par un nombre ou groupe de trois signes ou chiffres. Sachant d'ailleurs que n objets, combinés trois à trois de toutes les manières possibles, donnent $n \times n \times n = n^3$ permutations, nous reconnaissons que trois est la seule valeur qui puisse convenir à n ; deux ne donnerait que $2^3 = 8$ ternaires, tandis que quatre en fournirait $4^3 = 64$ et que trois en donne $3^3 = 27$.

Mais l'alphabet français ne contenant que vingt-six lettres, W compris, et le nombre des lettres devant forcément être égal à celui des groupes numériques, il est indispensable d'ajouter à l'alphabet une nouvelle lettre simple, le CH, le GN, Ä, Ë, Ö,... etc. pouvant occasionner des erreurs qu'il importe d'éviter. D'autre part le mélange des chiffres et des lettres étant prohibé en télégraphie, nous ne pouvons recourir qu'à un signe de ponctuation ou signe spécial ; le plus simple, pour l'exposé de la méthode, semble être la croix ou le signe arithmétique *plus*, +. Son emploi complétera notre alphabet, en portant à vingt-sept le nombre des lettres ; nous satisferons ainsi à la condition indispensable d'avoir autant de lettres que de combinaisons.

Croyant inutile de reproduire les détails déjà donnés au sujet des alphabets bifides, détails parfaitement applicables aux trifides, nous nous contenterons de présenter un alphabet du nouveau type et de l'appliquer au chiffrage d'une dépêche et à la traduction d'une seconde, en faisant ressortir les particularités intéressantes.

Alphabet Chiffrant		*Alphabet Déchiffrant*	
+ = 211	N = 111	111 = N	223 = D
A = 321	O = 323	112 = R	231 = L
B = 233	P = 132	113 = V	232 = T
C = 122	Q = 221	121 = W	233 = B
D = 223	R = 112	122 = C	311 = M
E = 212	S = 322	123 = G	312 = Z
F = 333	T = 232	131 = K	313 = I
G = 123	U = 133	132 = P	321 = A
H = 332	V = 113	133 = U	322 = S
I = 313	W = 121	211 = +	323 = O
J = 213	X = 331	212 = E	331 = X
K = 131	Y = 222	213 = J	332 = H
L = 231	Z = 312	221 = Q	333 = F
M = 311	»	222 = Y	»

Chiffrons la phrase suivante, après l'avoir divisée en groupes de *cinq* lettres, d'après des conventions supposées.

Nous commençons par inscrire *verticalement* sous chaque lettre, le groupe numérique qui lui correspond dans l'alphabet chiffrant; puis relevant *horizontalement*, trois à trois, les chiffres considérés comme écrits sur une seule ligne, nous en cherchons, dans l'alphabet déchiffrant, la valeur littérale que nous écrivons sous chaque colonne :

n e t' a t	*t e n d s*	*q u' a t o*	*i s e u l*
1 2 2.3 2	2 2 1.2 3	2 1 3.2 3	3 3 2.1 2
1.1 3 2.3	3.1 1 2.2	2.3 2 3.2	1.2 1 3.3
1 2.2 1 2.	2 2.1 3 2.	1 3.1 2 3.	3 2.2 3 1.
C A P Z E	Q B R Y P	J T O J G	H W J H L

La traduction se fait par l'opération inverse : on écrit d'abord les lettres secrètes par groupes dont l'importance est déterminée par les conventions, puis, cherchant dans l'alphabet chiffrant, la valeur de chacune des lettres, on inscrit *horizontalement* la valeur trouvée, en mettant un chiffre sous chaque lettre secrète jusqu'à la fin du groupe; on revient alors à la première lettre, qui reçoit un deuxième chiffre et, plus tard, un troisième. Ces

chiffres sont ensuite relevés *verticalement* et leur valeur littérale, donnée par l'alphabet déchiffrant, inscrite sous chaque colonne de chiffres, fournit la traduction cherchée.

Soit, pour exemple, une phrase de vingt lettres groupées par *sept*. Le dernier groupe ne contenant que six lettres, 2×3, est constitué par des trigrammes *fractionnés*, tandis que les deux autres ne renferment que des trigrammes *scindés*.

Ḣ Ḋ Ȧ J̇ +̇ Ḣ Ḃ	Q̇ Ṡ L̇ +̇ Ẋ Ḋ Ė	Ḣ J̇ Ė Ṙ U̇ Q̇
3 3 2 2 2 3 3	2 2 1 3 2 2 2	3 3 2 2 1 3
2 1 2 1 3 2 1	3 1 2 1 1 3 3	2 1 2 1 1 2
1 3 3 2 2 3 3	1 2 2 3 2 1 2	1 3 3 2 2 1
A i d e t o i	*l e c i e l t*	*a i d e r a*

L'alphabet chiffrant nous ayant fourni : H = 332, D = 223, A = 321..... nous écrivons :

Ḣ Ḋ Ȧ J + H B
3 3 2 2 2 3 3
2 1 . . . . .

le premier chiffre de A pouvant seul être inscrit à la première ligne, les deux derniers sont reportés à la deuxième et, pour éviter les erreurs, nous pointons chaque lettre après sa conversion en chiffres. Un peu d'exercice familiarisera promptement avec la méthode.

De même que les bigrammes, les trigrammes sont susceptibles d'être profondément modifiés par les *tours de clé multiples*, ainsi que par les *alphabets conjugués*. Le premier procédé mélange intimement les fragments de lettres et le second correspond au chiffrement, à l'aide d'un alphabet monolittéral, des cryptogrammes trigrammatiques.

Ces deux procédés peuvent être employés simultanément.

L'auteur du présent travail a annoncé, dans la *Cryptographie nouvelle* (Paris, Dubreuil, 1893), qu'il était possible de fragmenter les lettres en *quatre, six, neuf*..... parties. Une étude plus approfondie a permis de reconnaitre que c'est une erreur. Les lettres ne peuvent être rompues qu'en *deux, trois* ou *six* fragments et encore ces derniers forment-ils des quantités que les algébristes qualifient d'*imaginaires*.

Hexagrammes.

Les *hexagrammes* résultent de l'emploi d'un alphabet *bifide* conjugué avec un alphabet *trifide*.

Le premier rompt les lettres en *deux* fragments, qui sont, de

nouveau, brisés en *trois* parties par le second, soit en *sixièmes* ; mais ces sixièmes n'ont, jusqu'à présent, pu être déterminés et il n'est pas possible de leur attribuer une valeur réelle : il faudrait, pour cela, disposer d'un alphabet de soixante-quatre signes différents, le nombre des arrangements que peuvent prendre *deux* objets combinés six à six étant de $2^6 = 64$.

121	+	»	»	»	»	58	111	F
333	A	75	G	44	232	87	112	M
223	B	55	N	45	311	68	113	T
221	C	47	U	46	331	»	121	+
323	D	65	C	47	221	86	122	H
132	E	67	K	48	312	66	123	P
111	F	58	S	54	213	76	131	Y
232	G	44	B	55	223	67	132	E
122	H	86	L	56	321	88	133	O
212	I	84	V	57	322	78	211	Z
313	J	74	F	58	111	84	212	I
312	K	48	Q	64	222	54	213	S
321	L	56	D	65	323	47	221	C
112	M	87	P	66	123	64	222	Q
311	N	45	E	67	132	55	223	B
133	O	88	T	68	113	85	231	R
123	P	66	J	74	313	44	232	G
222	Q	64	A	75	333	77	233	X
231	R	85	Y	76	131	45	311	N
213	S	54	X	77	233	48	312	K
113	T	68	Z	78	211	74	313	J
331	U	46	I	84	212	56	321	L
322	V	57	R	85	231	57	322	V
233	X	77	H	86	122	65	323	D
131	Y	76	M	87	112	46	331	U
211	Z	78	O	88	133	»	332	W
332	W	»	»	»	»	75	333	A

L'alphabet ci-dessus a été divisé en trois séries, de manière à être, à la fois, chiffrant et déchiffrant et à permettre, en outre, la conversion directe des groupes binaires en groupes ternaires. La colonne médiane de chaque série a été, à cet effet, disposée dans l'ordre naturel.

Pour mieux différencier les groupes et éviter les chances d'erreur, on a fait usage, pour les alphabets bifides, des chiffres 4, 5, 6, 7 et 8, et, pour les trifides, de 1, 2 et 3.

Le chiffrement se fait selon les règles connues, avec cette seule différence que, au deuxième tour de clé, on substitue l'alphabet à trois chiffres à celui employé dès le début et qui

doit forcément être celui de deux chiffres, puisqu'il renfermera moins de lettres que le second.

Soit à cryptographier, en groupant par *sept* :

a u t r e f o	i s l e r a t	d e v i l l e
7 4.6 8.6 5 8	8 5.5 6.8 7 6	6 6.5 8.5 5.6
5.6 8.5 7.8 8.	4.4 6 7 5.5 8.	5.7 7.4 6 6 7.
J T D R T V O	R L M Q U A F	P F B D X U E

Ayant *bigraphié* à l'ordinaire, il nous reste à grouper par *sept*, ou par tout autre nombre convenu, et à *trigraphier* les lettres secrètes ci-dessus pour avoir le cryptogramme définitif :

J T D R T V O	R L M Q U A F	P F B D X U E
3 1 3.2 1 3.1	2 3 1.2 3 3.1	1 1 2.3 2 3.1
1 1.2 3 1.2 3	3 2.1 2 3 3 1	2 1.2 2 3.3 3
3.3 3 1.3 2 3.	1.1 2 2.1 3 1	3.1 3 3.3 1 2.
J S F R X U D	R X E P N H Y	M D + B A O K

Pour abréger et simplifier le travail, il vaut mieux, au lieu de chercher les lettres qui forment le cryptogramme *provisoire*, remplacer immédiatement chaque groupe de *deux* chiffres par le groupe de *trois* chiffres correspondant ; c'est-à-dire, au lieu de chercher la valeur de 74 = J, puis celle de J = 313, on lit directement, dans la deuxième série de l'alphabet : 74 = 313, et ainsi des autres : 68 = 113, 65 = 323, 85 = 231..... etc.

La traduction se fait par l'opération inverse de celle qui a servi à chiffrer.

On trouvera dans la *Cryptographie nouvelle*, sur les alphabets bifides et trifides, ainsi que sur les hexagrammes, beaucoup de détails qui ne peuvent trouver place ici.

Il semble cependant intéressant, pour montrer la valeur cryptographique des méthodes polygrammatiques, de faire ressortir par quelques chiffres la richesse infinie des combinaisons qui leur servent de base.

Les groupes binaires des alphabets bifides ne renferment que *cinq* chiffres différents ; chaque chiffre figure donc *dix* fois dans l'alphabet entier ou, ce qui revient au même, *dix fragments* de lettres différents sont représentés par le même chiffre ; un groupe de deux chiffres peut donc représenter 10 × 10 = 100 combinaisons différentes de fragments de lettres.

Les groupes ternaires des alphabets trifides n'étant formés que de *trois* chiffres, chacun de ceux-ci entre vingt-sept fois dans l'alphabet complet et, par suite, chaque groupe de trois chiffres formant une lettre peut être produit par 27 × 27 × 27 = 19.683 éléments différents.

Dans les hexagrammes, l'emploi simultané des alphabets bifides et trifides permet donc de représenter chaque lettre de 100 × 19.683 = 1 968 300 manières diverses.

Dans ce calcul, il n'est pas tenu compte de la dispersion des fragments de lettres, dispersion qui augmente la difficulté du déchiffrement sans clé dans des proportions si considérables que ce déchiffrement semble devoir être complètement impossible.

QUATRIÈME PARTIE

PROCÉDÉS AUXILIAIRES DE CHIFFREMENT

On appelle, d'après M. Valério (1), « procédés auxiliaires de » chiffrement, les moyens employés pour augmenter les chances » d'indéchiffrabilité des dépêches ».

Ces procédés tendent principalement à assurer *l'individualité des dépêches*, lorsqu'elles n'ont pas une longueur suffisante pour permettre au déchiffreur de les pénétrer sans de longues recherches, à moins qu'il ne parvienne à en collectionner un assez grand nombre pour que ses tâtonnements reposent sur une base solide.

Ces mêmes procédés doivent permettre, d'autre part, de *sectionner* les dépêches un peu étendues de manière à les transformer, pour ainsi dire, en une série de brèves, de telle sorte que toute répétition disparaisse et que rien ne puisse guider le travail du déchiffreur ennemi.

Ces résultats peuvent être obtenus par divers moyens, que nous étudierons successivement, et qui sont :

1° Groupements ;
2° Lettres nulles et lettres indices (lettres d'arrêt, lettres signes, lettres numériques) ;
3° Reports et déplacements ;
4° Clé variable, brisée ou multiple ;
5° Clé cryptographiée ;
6° Nombre-clé ;
7° Mot alphabétique ;
8° Mot d'ordre ;
9° Grilles transposantes et chiffrantes ;

(1) *De la Cryptographie*, 2e partie, page 50. Baudoin, Paris, 1896.

Nous nous occuperons ensuite de la conversion en lettres des nombres et des signes de ponctuation, puis du chiffrement en chiffres arabes.

1° **Groupements.** — Nous avons vu que le groupement, nécessaire pour certaines méthodes de transposition, est utile pour le *fractionnement des bigrammes fixes* et indispensable pour l'obtention des *polygrammes scindés*.

Son emploi avec les *systèmes alphabétiques* permet de changer fréquemment de clé et, par suite, de transformer un texte clair d'une certaine longueur en une série de cryptogrammes courts et indépendants les uns des autres, en apparence du moins.

Le *groupement* consiste dans la séparation du texte clair en groupes de lettres plus ou moins nombreuses ; ces groupes sont déplacés ou cryptographiés isolément, suivant une loi convenue. Les nombres de lettres qu'ils renferment peuvent être, selon les cas et la loi de formation, égaux ou inégaux ; ils peuvent être fixes, déterminés par des occurrences diverses ou variables selon le caprice du chiffreur.

La valeur de chaque groupe peut être déterminée par des nombres fixes convenus ou variables et formant une série indéfinie, ainsi que nous l'avons exposé, page 26, au sujet de la première méthode de M. le colonel Roche, soit par la valeur numérique des lettres de la clé, soit par l'apparition d'une lettre convenue, soit par la rencontre d'une même lettre dans le texte et dans la clé... etc., soit par l'introduction d'une lettre spéciale.

Ainsi, nous pouvons convenir d'arrêter le premier groupe à cinq lettres, le deuxième à neuf, le troisième à onze, etc., ou de prendre pour la valeur des groupes successifs chacun des chiffres significatifs du quotient, ou du reste, de la division de deux nombres, $\frac{m}{n}$ comme $\frac{1}{7} = 0{,}1428571$. Nous pouvons, de même, avec la clé CHIEN, par exemple, dont les lettres occupent les troisième, huitième, neuvième, cinquième et quatorzième rangs dans l'alphabet normal, faire des groupes de trois, huit, neuf, cinq et quatorze lettres ; au lieu de prendre l'ordre alphabétique normal, on peut prendre l'ordre dans un alphabet interverti. On peut également terminer les groupes à une lettre de grande fréquence, telle que E, A, S, I, N, T, R ; soit E la lettre choisie, la phrase :

Je | *vous atte* | *nds de* | *main*, sera divisée en quatre groupes respectivement de deux, huit, cinq et quatre lettres. Enfin, le terme des groupes peut être indiqué par l'insertion d'une lettre convenue, à des endroits quelconques au choix du chiffreur.

2° **Lettres nulles et lettres indices.** — Les lettres *nulles*, ou non-valeurs, sont des lettres intercalées dans le texte clair ou

dans le texte chiffré et destinées soit à compléter un groupe, soit simplement à dérouter le déchiffreur. Elles sont parfois, mais rarement, utiles, jamais indispensables. Leur emploi présente toujours l'inconvénient de compliquer le travail du chiffreur, ainsi que celui du traducteur, sans augmenter sensiblement les chances de secret, souvent même en les diminuant, par exemple, dans la méthode dite des diviseurs. Il convient donc de les rejeter, en principe.

Les *lettres indices* servent à définir une opération prévue par les conventions, mais non entièrement précisée. Parfois la lettre indice, dite alors *lettre d'arrêt*, sert, par sa seule présence, à indiquer la fin des groupes dont l'importance est laissée à la volonté de l'expéditeur (système des arrêts variables).

M. de Viaris fait usage d'une lettre indice tant pour déterminer le type de grille employée, que pour indiquer l'augment dont il fait usage dans son système autoclave.

Nous verrons plus loin le mode d'emploi des lettres signes pour les nombres et la ponctuation.

Nous aurons souvent besoin de *lettres numériques* pour définir quelques opérations. Le système qui nous semble le meilleur consiste à indiquer le nombre à transmettre, dans ces cas particuliers, par la lettre dont le numéro d'ordre est égal à ce nombre, dans l'alphabet dont on fait usage, en commençant à compter depuis l'origine pour les nombres positifs et à compter de la dernière lettre pour les nombres négatifs.

3° **Reports et déplacements.** — Les *déplacements* sont de simples transpositions de groupes, opérées avant ou après le chiffrement. Bien effectués, ils peuvent, sans complication gênante, augmenter considérablement les garanties du secret; nous en avons donné plusieurs exemples en étudiant les bigrammes fractionnés.

Le *report* est un déplacement d'un genre spécial; il a surtout pour but d'opposer un obstacle sérieux, sinon insurmontable, au déchiffrement de certaines dépêches chiffrées avec les systèmes alphabétiques, mais trop courtes pour qu'on puisse leur appliquer utilement les principes usuels de la cryptophotie.

« Si, dit M. Kerckhoffs (1), dans le déchiffrement d'un crypto-
» gramme à alphabets intervertis, il est impossible de déter-
» miner le nombre des alphabets de la clé, soit parce que la
» dépêche est trop courte, soit parce que la clé est trop longue,
» la solution du problème présente des difficultés, sinon insur-
» montables, du moins capables de lasser la patience du plus
» habile déchiffreur.

(1) *La Cryptographie militaire*. Baudoin, Paris, 1883.

» La situation change si l'on se trouve en possession de » plusieurs cryptogrammes écrits avec la même clé, si courts » qu'ils soient d'ailleurs ; en les ordonnant les uns au-dessous » des autres, on peut faire sur la répétition des lettres un calcul » analogue à celui que nous avons fait sur les chiffres groupés » par tranches ou par colonnes. »

Le *report* met un obstacle absolu à l'application de l'ingénieuse méthode imaginée par M. Kerckhoffs, car cette opération dissimule complètement le *début réel* de la dépêche. Elle consiste, en effet, à reporter de la fin au commencement, ou du commencement à la fin, une partie des chiffres de la dépêche.

Le nombre essentiellement variable des lettres reportées est fixé par le chiffreur, qui le fait connaître à son correspondant à l'aide de lettres numériques dites *lettres de report*.

Exemple : Un chiffreur veut reporter, de la fin au commencement, les *cinq* derniers chiffres de sa dépêche ; en supposant que, dans l'alphabet dont il s'est servi, N occupe la cinquième place et K la vingt-deuxième (alphabet de vingt-six lettres), les lettres de report seront : N = + 5 et K = — 5 et la dépêche devra commencer par K suivi des *cinq* dernières lettres, puis du reste de la dépêche et de N remplaçant les cinq lettres reportées. Au contraire, commencer la dépêche par N et la terminer par K serait indiquer qu'il faut reporter les cinq lettres précédant K au commencement de la dépêche, dont on supprime N. En un mot, N indique qu'il faut ajouter cinq lettres et K qu'il faut en supprimer le même nombre. Pour éviter toute ambiguïté, les lettres de report doivent occuper les places extrêmes de la dépêche.

Malgré sa simplicité et sa facilité d'application, le report ne laissera pas de créer des difficultés nouvelles pour les déchiffreurs, mais non pour les traducteurs.

4° **Clé variable, brisée ou multiple.** — Afin de rendre plus difficile la découverte du nombre de lettres composant la clé, ce qui facilite beaucoup le déchiffrement, on a eu l'ingénieuse idée d'arrêter, à des intervalles irréguliers, l'ordre de succession des alphabets employés pour revenir brusquement à la lettre initiale. On indique le point d'arrêt par une lettre indice ou *lettre d'arrêt*.

Au lieu de revenir au premier alphabet indiqué par la clé, on peut aussi, après la lettre d'arrêt, changer complètement ou partiellement la clé. Soient, par exemple, EPAMINONDAS, la clé générale et W, la lettre d'arrêt ; convenons de prendre pour clés successives, trois lettres seulement de la clé générale, en commençant par EPA et, après l'insertion de la lettre indice W, de rejeter la première lettre E, et d'ajouter la quatrième M, et

ainsi de suite. Nous aurons avec EPAMINONDAS, une série de onze clés : EPA, PAM, AMI, MIN, INO, NON, OND, NDA, DAS, ASE, SEP, de trois lettres, dont chacune est appliquée à un groupe plus ou moins long, à la volonté de l'expéditeur.

Dans les procédés ci-dessus, les groupes régis par chaque clé réduite sont déterminés par une lettre d'arrêt, chiffrée ou non. Le groupement peut être fixé par convention ; il peut même résulter de la forme de la clé ; ainsi prenons une phrase facile à retenir : *Aux petits des oiseaux Dieu donne la pâture* ; convenons que chaque mot sera successivement employé trois fois de suite comme clé et nous pourrons cryptographier cent-huit lettres, savoir : neuf avec *aux*, dix-huit avec *petits*, neuf avec *des*, vingt et une avec *oiseaux*, etc., sans avoir de répétitions de chiffres susceptibles de fournir des renseignements utiles pour le déchiffrement.

5° **Clé cryptographiée.** — Un moyen simple et d'une valeur indéniable d'assurer l'individualité des dépêches consiste à laisser le *choix de la clé à l'expéditeur*.

On obtient ce résultat, en faisant précéder le texte clair du *mot d'ordre*, généralement employé comme clé, et en chiffrant ensuite le tout avec un nouveau mot, qui n'est astreint qu'à l'unique condition d'avoir, au plus, autant de lettres que le mot d'ordre. Quand la clé choisie en possède un nombre moindre, le fait doit être signalé par l'insertion d'une ou de plusieurs lettres d'arrêt.

Il est utile de remarquer que la clé ainsi cryptographiée n'étant pas, par sa nature même, destinée à être conservée puisque son emploi se réduit à chiffrer une *seule et unique* dépêche, peut être composée de lettres ne présentant aucun sens, et qu'elle échappe ainsi aux méthodes de déchiffrement basées, comme celle du major Kasiski, sur la détermination de la clé.

Cryptographions la dépêche : *Nous partirons demain*.

La méthode convenue est celle de Gronsfeld ; le mot d'ordre est AGE=064. Nous opérons comme suit :

AGE	*n o u*	*s p a*	*r t i*	*r o n*	*s d e*	*m a i*	*n*
3 2 1	3 2 1	3 2 1	3 2 1	3 2 1	3 2 1	3 2 1	3
D I F	Q Q V	V R B	U V J	U Q O	V F F	P C J	Q

Le correspondant, sachant que DIF est le cryptogramme de AGE, n'éprouvera aucune difficulté à en déduire la clé, on a, en effet :

$$\begin{cases} \text{D I F} - \text{A G E} = \text{D C B} \\ 3\,8\,5 - 0\,6\,4 = 3\,2\,1 \end{cases}$$

De même que les clés *claires*, les clés cryptographiées peuvent être brisées et modifiées de toute façon. On peut même ne pas augmenter le nombre des lettres de la dépêche, en prenant pour clé réelle le début de cette même dépêche; dans le cas ci-dessus, on aurait, avec le chiffre de Vigenère :

n o u	*s p a*	*r t i*	*r o n*	*s d e*	*m a i*	*n*
A G E	n o u	n o u	n o u	n o u	n o u	n
N U Y	F D U	E H C	E C H	F R Y	Z O C	A

6° **Nombre-clé.** — On peut même supprimer le mot d'ordre, en convenant de prendre pour clé particulière à chaque dépêche un nombre indiqué par une lettre *numérique*.

Ainsi, pour indiquer, avec l'alphabet normal, que nous avons cryptographié avec le mot *quatorze* pour clé, nous nous contenterons de faire précéder notre dépêche de la lettre N, qui occupe le quatorzième rang dans l'alphabet.

Soit maintenant à traduire une dépêche, *avec report*, chiffrée à l'aide du tableau de la page 37, qui a pour base l'alphabet : KLAGENFURTH....., etc,

F F M Q Z V B F K D N F L O U S T L H Q I E H Q N R M V Q

La première et la dernière lettre sont des *lettres de report* et ne font pas partie intégrante de la dépêche; F=+7 et Q=—7, ce qui signifie que les *sept* dernières lettres doivent être reportées de la fin au commencement; mais, après cette opération, la première lettre, E, doit encore être supprimée comme *lettre numérique* indiquant la clé, qui est CINQ, la lettre E occupant le cinquième rang dans l'alphabet convenu, de même que F et Q occupent les septième et vingtième rangs. Nous aurons finalement :

Clé :	HQNR	MVFM	QZVB	FKDN	FLOU	STLH	QI
E = cinq.	c i n q	c i n q	c i n q	c i n q	c i n q	c i n q	c i
	i l s s	*o n t a*	*r r i v*	*é s a p*	*e t e r*	*s b o u*	*r g*

Ici encore, nous pouvons faire usage de clés variables et même indéfinies, le nombre indiqué par la lettre numérique étant considéré comme le premier d'une série arithmétique convenue, telle que : 5, 6, 7, 8, 9, 10, 11, 12..., ou 5, 8, 11, 14 ..., etc., dont chaque terme, après avoir été employé deux ou trois fois, sera remplacé par le suivant. Il convient cependant de faire remarquer que, à partir de 20, il y a inconvénient à employer plusieurs fois le même nombre comme clé et à lui substituer des nombres trop voisins, à cause de la répétition des noms de dizaines : vingt, trente, quarante..., etc.

La lettre numérique peut être doublée et les deux nombres, ainsi transmis, servir à une opération arithmétique fournissant la vraie clé.

Ces mêmes lettres peuvent, par conventions, s'appliquer à une nomenclature quelconque et donner de nouvelles clés : les mois, les jours de la semaine, les couleurs du spectre, les éléments, les planètes, etc., etc.

7° **Mot alphabétique.** — Le chiffrement par polygrammes ne paraît pas avoir besoin de clé, sauf pour les groupements, toutes les opérations se faisant avec un alphabet bifide ou trifide, ou avec un damier dont chaque correspondant doit être muni et qu'aucune clé ne semble pouvoir modifier.

Il est cependant facile d'assurer l'individualité des dépêches de cette nature par les moyens suivants.

Chaque correspondant étant en possession d'un alphabet bifide ou trifide, ou, ce qui revient au même, d'un carré alphabétique, le chiffreur commence sa dépêche en cryptographiant, selon les conventions, le mot ou les indications spéciales qui doivent servir à la formation d'un nouvel alphabet, suivant les règles établies.

Avec les alphabets à deux ou trois chiffres, ce nouvel alphabet pourra servir d'alphabet conjugué. Avec les carrés, il formera, suivant la place qu'il doit occuper d'après les conventions, un demi-damier vertical ou horizontal. Dans tous les cas, la dépêche pourra être chiffrée avec des documents individuels.

Lorsque le damier commun aux correspondants doit être complet, on se servira pour l'envoi du *mot alphabétique* des deux alphabets principaux disposés en un demi-damier vertical, qui correspond au damier normal complet, et les premières indications de la dépêche auront pour objet d'assigner leurs places aux lignes et aux colonnes des alphabets auxiliaires.

Le même procédé peut être utilisé pour la formation des bandes dans les systèmes alphabétiques et nous avons vu que, rapproché de l'alphabet primitif, normal ou conventionnel, ce dernier nous fournira, sans compter les sous-alphabets, cent quatre nouveaux alphabets, par l'emploi raisonné des formules cryptographiques.

8° **Mot d'ordre.** – Le *mot d'ordre*, dénommé jusqu'ici *mot-clé*, à cause de son usage, ne doit servir qu'à la formation de l'alphabet *primitif*, c'est-à-dire de celui qui sert aux correspondants à fixer les clés et les alphabets spéciaux à chaque dépêche, ainsi qu'il est exposé dans les divers paragraphes ci-dessus.

Il peut se faire, en effet, qu'une dépêche isolée, très courte et habilement composée, soit indéchiffrable, tandis que le même système ne donnera aucune sécurité dans un service régulier,

celui de l'armée, par exemple, où des milliers de dépêches sont écrites avec le même système et souvent avec la même clé.

Il importe donc *d'individualiser* chaque dépêche et, par suite, de restreindre au strict nécessaire l'emploi des bases communes et de dissimuler ces bases autant que faire se peut.

C'est ce qui nous a amené à étudier les procédés auxiliaires de chiffrement. Bien d'autres méthodes pourront être imaginées dans le même but, mais celles qui précèdent rendront toujours de réels services.

9° **Grilles transposantes et chiffrantes.** — Nous avons déjà indiqué quelques moyens d'augmenter les garanties qu'offre l'emploi des grilles. Cependant ces garanties nous paraissant encore insuffisantes, nous avons cherché un moyen pratique de mélanger, à l'aide des grilles, les deux systèmes cryptographiques de transposition et de substitution.

A cet effet, nous attribuons à chaque fenêtre un chiffre simple, que nous employons comme une clé du système de Gronsfeld. Par suite du mélange des lettres opéré par la grille, les clés numériques se suivent sans ordre apparent et peuvent, en conséquence, être peu nombreuses. Divisons, par exemple, notre grille en quatre quartiers et donnons à chacun d'eux un chiffre différent, soit : deux, trois, quatre, cinq. La lettre qui devra être inscrite dans une des fenêtres du carré côté deux sera remplacée par celle qui vient *deux* rangs après elle dans l'alphabet normal, et ainsi des autres. Nous pouvons également attribuer un chiffre à chaque position de la grille, etc.

Tel est le principe qui est susceptible de nombreuses modifications et de nature à rendre le déchiffrement à peu près impossible sans, pour cela, augmenter les difficultés de la traduction.

Au lieu de recourir au système de Gronsfeld, on peut faire usage de deux bandes alphabétiques et chiffrer chaque lettre avant de l'inscrire dans l'ouverture de la grille qui lui est destinée.

Exemple : Chiffrons les premières lettres de l'alphabet normal avec la grille ci-dessous, employée par rotation (première manière), en faisant usage, à chaque rotation, de la clé littérale placée à chaque angle :

R V 1 2 3 4 Y S

Les chiffres indiquent l'ordre d'inscription des lettres dans toutes les positions de la grille.

Nous aurons le cryptogramme suivant, où les majuscules représentent les lettres du texte, et les minuscules les clés qui doivent servir à les chiffrer :
P*y*, F*v*, A*r*, L*s*, E*v*, O*y*. K*s*, B*r*, J*s*, C*r*, G*v*, M*y*, D*r*, I*s*, N*y*, H*v*

Ici encore, le choix des clés peut être laissé à la discrétion de l'expéditeur, qui les inscrira dans sa dépêche même, par un des moyens déjà exposés.

Si nous avions chiffré chaque lettre avant de l'inscrire dans les fenêtres de la grille, nous aurions eu avec le tableau de la page 37, en faisant précéder la dépêche des *chiffres* de la clé, pris dans l'alphabet A, le cryptogramme suivant :

OVPY DKOGZCAPLQLHSKBA
au lieu de : RVSY *a b c d e f g h i j k l m n o p*

Représentation des signes numériques et orthographiques.

Note. — Le présent paragraphe est extrait de *L'Art de chiffrer et déchiffrer les dépêches secrètes*, par le savant et regretté marquis de Viaris, récemment enlevé à la science cryptographique, dont il était un des maitres les plus autorisés.

Nécessité d'une convention. — Il peut arriver que, dans le courant d'une dépêche, on ait absolument besoin d'indiquer la ponctuation ou l'orthographe exacte d'un nom propre ; à coup sûr il arrivera que l'on ait à parler de nombres qu'il serait trop long de traduire en toutes lettres ; quel que soit le système employé, une convention s'impose.

Représentation des chiffres arabes et des nombres. — Voici celle que nous proposons. Les dix chiffres arabes seront représentés par les dix premières lettres de l'alphabet :

A	B	C	D	E	F	G	H	I	J
1	2	3	4	5	6	7	8	9	0

et, pour avertir de leur signification numérique, on les encadrera entre deux K, ainsi KCK signifiera 3, et KCFIJAK : 36.901.

Les signes orthographiques. — Toutes les autres lettres de l'alphabet placées comme les dix premières entre deux K auront une signification de signes orthographiques :

L	M	N	O	P
virgule	point	alinéa	exclamation	interrogation
,	.		!	?

Q	R	S	T	U	V
guillemets	parenthèse	trait d'union	apostrophe	cédille	tréma
»	( )	-	'	¸	¨

X	Y	Z
accent aigu	accent grave	accent circonflexe
´	`	^

Les signes relatifs aux nombres. — Mais on peut aussi, sans crainte de confusion, placer l'une de ces lettres entre deux des dix premières ou entre l'une d'elles et un K et alors lui donner une signification différente et ayant rapport aux signes numériques. L signifierait « virgule » comme ci-dessus et 25,33 se traduirait par KBELCCK. Les autres lettres voudraient dire :

Q	R	S	T	U
numéro	terminaison ième	séparation de deux nombres	terminaison ièmement	exposant ou puissance

V	X	Y	Z
plus	moins	multiplié par	divisé par ou barre de fraction
+	—	×	

Les lettres M N O P restent disponibles si l'on avait à établir d'autres conventions relatives aux nombres.

Donnons quelques exemples :

Numéro 27 :	K Q B G K
Vingt-septième :	K B G R K
27—32—14 :	K B G S C B S A D K
Vingt-septièmement :	K B G T K
27^4 :	K B G U D K
27 plus 32 :	K B G V C B K
32 moins 27 :	K C B X B G K
32 multiplié par 27 :	K C B Y B G K
32 divisé par 27 :	K C B Z B G K, etc.

Dans les conventions précédentes, nous n'avons pas parlé du point et virgule (;) qui se traduira par K M L K, ni des deux points (:) que l'on traduira par K M M K.

De Viaris. — *L'art de chiffrer*, etc.

Note. — Les lettres M N O P, laissées disponibles par M. de Viaris, peuvent être employées pour indiquer le mode de *décimation des alphabets*. Elles pourraient prendre les valeurs suivantes :

M	N	O	P
décimation directe par	décimation inverse par	origine de la décimation	nombre de lettres de l'alphabet

Exemples : décimation directe par 7, première lettre ou origine de la décimation : H, alphabet de vingt-cinq lettres : K M G O H P B E K ; décimation inverse par 9, première lettre décimée : D, alphabet de vingt-six lettres : K N I O D P B F K. Enfin le W peut indiquer les groupements : K W G K = groupez par 7.

Numération par 25. — Lorsqu'il s'agit de grands nombres on peut recourir à la numération par 25 en se servant, en guise de caractères arithmétiques, des lettres de l'alphabet : A = 0, B = 1. . . . Y = 24, que l'on encadre avec W ou Z.

Exemple : W P E R I L W = $15 \times 25^4 + 4 \times 25^3 + 17 \times 25^2 + 8 \times 25 + 11 =$
(P = 15, E = 4, R = 17, I = 8, L = 11)

5.932.711. Un barème, facile à établir, rendra les calculs simples et rapides en réduisant le chiffrement à une courte addition et la traduction à des soustractions.

Conversion des lettres en chiffres arabes. — Les conventions télégraphiques internationales prohibant les cryptogrammes littéraux, il y a lieu de les modifier et de les transformer en chiffres arabes. A notre connaissance, deux méthodes ont été proposées à cet effet :

1° *Méthode anglaise.* — Attribuer les cent premiers nombres de 00 à 99, aux lettres de l'alphabet, en donnant à chaque lettre une quantité de nombres en rapport avec sa fréquence.

La longueur de la liste numéro-alphabétique doit rendre la traduction très pénible. En outre, cette méthode présente l'inconvénient de doubler les signes à transmettre, puisque chaque lettre est représentée par deux chiffres.

2° *Méthode de M. de Viaris.* — Dans cette méthode, les lettres usuelles, augmentées de certaines lettres accentuées, sont divisées, suivant leur fréquence, en trois séries. Dans la première, chaque lettre reçoit un chiffre, qui la représente ; les lettres correspondantes des deuxième et troisième séries sont représentées respectivement par le même chiffre répété deux ou trois fois.

Le nombre des chiffres à transmettre n'est plus que de cent trente-cinq pour cent lettres, mais on se trouve dans l'obligation de supprimer les lettres doubles, ce qui ne laisse pas de nuire à la clarté des dépêches.

Nous avons cherché à remédier aux défectuosités de ces mé-

thodes et nos recherches nous ont conduit aux observations suivantes :

Dans un chapitre précédent, nous avons étudié une méthode (Méthode Auvray, page 45) dont les cryptogrammes sont formés de chiffres arabes ; mais le nombre de ces chiffres étant variable pour chaque lettre, cette méthode ne peut, sans modifications, être employée dans les communications télégraphiques.

En remplaçant, dans un damier complet, les lettres de chacun des alphabets auxiliaires par les groupes numériques d'un alphabet bifide, on obtient des bigrammes en chiffres arabes, mais le nombre de ces chiffres est toujours double de celui des lettres.

Pour réduire au *minimum* le nombre des chiffres nécessaires, il faut avoir recours à l'un des moyens ci-après indiqués :

Alphabets numériques. — En numérotant, de 0 à 26, les lettres de l'alphabet, il faut employer quarante-deux chiffres ; la méthode suivante en exige quarante-quatre, soit deux de plus seulement.

Choisir deux chiffres, dits *chiffres de dizaines*, qui ne pourront représenter une lettre que suivis d'un second chiffre ; les huit autres, dits *chiffres d'unités* pourront être employés seuls ou placés *à droite* d'un chiffre de dizaines ; enfin l'un ou les deux chiffres de dizaines pourront jouer le rôle de chiffres d'unités pouvu qu'ils soient eux-mêmes précédés d'un chiffre de dizaines.

Afin de diminuer autant que possible le nombre des caractères des cryptogrammes, nous représenterons par les *chiffres des unités* huit des dix lettres de plus grande fréquence, savoir : E, A, S, I, N, T, R, U, L, O ; les autres auront pour valeur un nombre de deux chiffres.

Formons un alphabet en prenant 0 et 1 pour chiffres de dizaines :

Alphabet Chiffrant.			*Alphabet Déchiffrant.*		
A = 6	J = 19	S = 2	»	01 = K	11 = D
B = 03	K = 01	T = 3	2 = S	02 = P	12 = M
C = 17	L = 04	U = 7	3 = T	03 = B	13 = F
D = 11	M = 12	V = 08	4 = E	04 = L	14 = H
E = 4	N = 5	W = 16	5 = N	05 = G	15 = Y
F = 13	O = 06	X = 09	6 = A	06 = O	16 = W
G = 05	P = 02	Y = 15	7 = U	07 = Z	17 = C
H = 14	Q = 18	Z = 07	8 = I	08 = V	18 = Q
I = 8	R = 9	»	9 = R	09 = X	19 = J

Cryptographions les mots : *République française.*

r e p u b l i q u e f r a n ç a i s e.... 19 lettres
9 4 02 7 03 04 8 18 7 4 13 9 6 5 17 6 8 2 4.... 25 chiffres

Pour bien montrer qu'il ne peut y avoir confusion entre les valeurs numériques d'un ou de deux chiffres, traduisons la dépêche ci-dessous :

04455 78561 87837 51906 79114 04758 13069 12834

Nous commençons par marquer tous les groupes binaires du cryptogramme, en réunissant par un tiret, placé au-dessus ou au-dessous, les chiffres de dizaines, 0 et 1, et le chiffre placé à droite ; puis, à l'aide de l'alphabet déchiffrant, nous inscrivons, sous chaque chiffre ou groupe, sa valeur littérale :

$\overline{04}$ 4 5 5 7 8 5 6 $\overline{18}$ 7 8 3 7 5 $\overline{19}$ $\overline{06}$ 7 9 $\overline{11}$ 4 $\overline{04}$ 7 5 8 $\overline{13}$ $\overline{06}$ 9 $\overline{12}$ 8 3 4
l e n n u i n a q u i t u n j o u r d e l u n i f o r m i t e

Remarquons qu'il reste encore deux groupes binaires disponibles : 00 et 10, qui peuvent être employés comme signes de ponctuation, ou représenter des lettres doubles, accentuées, etc.

Cet alphabet étant monolittéral, puisque chaque lettre est représentée par un nombre invariable, il convient, pour assurer le secret, de recourir aux procédés auxiliaires déjà connus, ou mieux, puisque nous avons affaire à des chiffres, à une opération arithmétique quelconque.

L'addition et la soustraction d'une série numérique illimitée : suite naturelle des nombres, suite des nombres pairs ou impairs, progression arithmétique ou géométrique, fraction décimale, etc., dénaturent les dépêches d'une manière capable d'assurer le secret.

Il en est de même de la multiplication d'un cryptogramme par un nombre quelconque, mais de préférence inférieur à 10, afin de faciliter les calculs et d'éviter l'introduction de plusieurs chiffres nouveaux.

La division peut aussi être employée, mais le travail est moins facile et il y a quelques précautions à prendre, notamment pour l'indication du reste de la division.

L'emploi d'une opération arithmétique n'exclut pas le recours aux procédés auxiliaires, tels que : transposition de groupes, reports, mots alphabétiques, grilles transposantes et chiffrantes, etc., etc.

Nous verrons plus loin une nouvelle méthode *semi-bigrammatique* à laquelle conduit le présent système.

Carré numérique. — Les dix chiffres usuels, combinés *trois à trois* fournissent $10 \times 10 \times 10 = 1.000$ arrangements : 000 à 999. Les vingt-six lettres de l'alphabet, combinées *deux à deux* ne donnent que $26 \times 26 = 676$ bigrammes ; *deux* lettres peuvent donc toujours être représentées par *trois* chiffres.

La seule difficulté réside dans la longueur de la liste et la lenteur des recherches qu'elle occasionne. Mais, en disposant les nombres en un carré bordé de deux alphabets, la recherche des nombres correspondant à un bigramme déterminé devient facile puisque ce nombre est à l'intersection de la rangée appartenant à l'une des lettres du bigramme et de la colonne ressortissant à l'autre lettre. Le travail est donc le même que pour l'emploi d'un chiffre carré et il présente sur celui-ci l'avantage de chiffrer deux lettres à la fois, comme les tableaux de bigrammes.

Un peu d'arithmétique est indispensable avant d'entreprendre la formation de notre carré numérique.

$1.000 = 676 + 324$ ou $1.000 = 26^2 + 18^2$; $1.000 = 900 + 100 = 30^2 + 10^2$; on a encore : $1.000 = 25 \times 40$ et $1.000 = 31^2 + 39$ ou enfin $= 31 \times 32 + 8$.

D'autre part, nous pouvons employer des alphabets de vingt-cinq ou vingt-six lettres ; nous pouvons même en composer de trente et un, trente-deux et quarante caractères, en ajoutant aux lettres, soit les chiffres arabes, les signes de ponctuation ou d'accentuation, soit quelques bigrammes ou trigrammes d'un emploi fréquent, soit enfin des mots entiers d'un usage journalier. Nous pouvons enfin réserver jusqu'à 375 $(= 1.000 - 625)$ nombres pour faire un répertoire.

Il en résulte de nombreuses combinaisons présentant chacune ses avantages et aussi ses inconvénients, mais leur étude sortirait des limites que nous nous sommes tracées. Nous nous contenterons donc, après avoir exposé en détail la méthode qui nous semble réunir le plus de garantie et de simplicité, de donner quelques renseignements sur une seconde méthode susceptible de fournir certains avantages.

Carré numérique complet à origine variable. — Ce tableau, formé de trente-deux lignes et de trente-deux colonnes, dont l'une ne contient que huit nombres $(1.000 = 31 \times 32 + 8)$, peut être utilisé de diverses manières ; nous n'exposerons que la plus simple.

On remplit chacune des mille cases de ce tableau, en y inscrivant l'un des nombres de 000 à 999, en ayant soin de compléter par des zéros, placés à gauche, les nombres de la première centaine pour les transformer en ternaires. S'il est indispensable de suivre les nombres dans leur ordre naturel, il est insignifiant d'inscrire cet ordre par rangées ou par colonnes, autrement dit verticalement ou horizontalement.

Dans le tableau ci-après, nous suivrons l'ordre vertical et consacrerons la trente-deuxième colonne aux huit derniers ternaires, auxquels nous pourrions attribuer les valeurs suivantes : 992 = *virgule*, 993 = *point*, 994 = *tiret*, 995 = *point d'interrogation*, 996 = *tréma*, 997 = *accent aigu*, 998 = *accent grave*, 999 = *accent circonflexe*.

Ce tableau n'exige pas le secret et peut, sans nul inconvénient, être mis dans le commerce et laissé dans toutes les mains puisque, pour la facilité des recherches, on a suivi, dans sa confection, l'ordre naturel des nombres.

Pour rendre son maniement plus commode, il est bon de le coller sur une planchette à charnières ou sur un carton fort pouvant se replier en deux, afin d'en rendre le transport plus facile.

Deux bandes alphabétiques sont indispensables pour son emploi : l'une verticale et l'autre horizontale. Leurs alphabets peuvent être intervertis ou non La bande horizontale se place en bordure du tableau, ou sur l'une des six premières rangées; la bande verticale se place en bordure du tableau, ou sur l'une des cinq premières colonnes, de telle sorte que l'un des quarante-deux nombres compris dans le petit rectangle tracé à la partie *supérieure gauche* du tableau se trouve dans l'angle droit formé par le croisement des deux bandes et corresponde au bigramme composé par la première lettre de chacun des alphabets. Ce nombre est la *clé numérique*.

Il est facile d'imaginer un moyen de fixer les bandes alphabétiques à la place choisie : de petits crampons en fil de cuivre recourbé insérés sur les traits qui séparent les carrés numériques, un ressort sur le pourtour du tableau et même, à défaut d'autre chose, une épingle ou une punaise enfoncée dans la tranche du carton-support, etc.

Cependant pour chiffrer les mots : *République française*, afin de ne cacher aucune partie du tableau, nous posons les alphabets conventionnels dans les bordures, au lieu de recouvrir la quatrième rangée avec l'alphabet horizontal et la troisième colonne avec l'alphabet vertical, mais nous les disposons de manière que la *clé numérique* choisie, 100, soit le chiffre correspondant au bigramme formé par la première lettre de chacun des alphabets ; ce bigramme sera HJ ou JH, selon que la première lettre des bigrammes sera lue dans l'alphabet horizontal ou dans l'alphabet vertical.

Adoptons ce dernier système et chiffrons :

re	pu	bl	iq	ue	fr	an	ca	is	ew
315	839	229	893	304	425	760	682	829	210

				H	D	B	W	L	O	E	I	F	T	R	C	M
	000	032	064	096	128	160	192	224	256	288	320	352	384	416	448	480
	001	033	065	097	129	161	193	225	257	289	321	353	385	417	449	481
	002	034	066	098	130	162	194	226	258	290	322	354	386	418	450	482
	003	035	067	099	131	163	195	227	259	291	323	355	387	419	451	483
J	004	036	068	100	132	164	196	228	260	292	324	356	388	420	452	484
B	005	037	069	101	133	165	197	229	261	293	325	357	389	421	453	485
V	006	038	070	102	134	166	198	230	262	294	326	358	390	422	454	486
P	007	039	071	103	135	167	199	231	263	295	327	359	391	423	455	487
Y	008	040	072	104	136	168	200	232	264	296	328	360	392	424	456	488
F	009	041	073	105	137	169	201	233	265	297	329	361	393	425	457	489
C	010	042	074	106	138	170	202	234	266	298	330	362	394	426	458	490
X	011	043	075	107	139	171	203	235	267	299	331	363	395	427	459	491
K	012	044	076	108	140	172	204	236	268	300	332	364	396	428	460	492
N	013	045	077	109	141	173	205	237	269	301	333	365	397	429	461	493
H	014	046	078	110	142	174	206	238	270	302	334	366	398	430	462	494
S	015	047	079	111	143	175	207	239	271	303	335	367	399	431	463	495
U	016	048	080	112	144	176	208	240	272	304	336	368	400	432	464	496
Q	017	049	081	113	145	177	209	241	273	305	337	369	401	433	465	497
E	018	050	082	114	146	178	210	242	274	306	338	370	402	434	466	498
D	019	051	083	115	147	179	211	243	275	307	339	371	403	435	467	499
L	020	052	084	116	148	180	212	244	276	308	340	372	404	436	468	500
W	021	053	085	117	149	181	213	245	277	309	341	373	405	437	469	501
O	022	054	086	118	150	182	214	246	278	310	342	374	406	438	470	502
G	023	055	087	119	151	183	215	247	279	311	343	375	407	439	471	503
A	024	056	088	120	152	184	216	248	280	312	344	376	408	440	472	504
Z	025	057	089	121	153	185	217	249	281	313	345	377	409	441	473	505
T	026	058	090	122	154	186	218	250	282	314	346	378	410	442	474	506
R	027	059	091	123	155	187	219	251	283	315	347	379	411	443	475	507
M	028	060	092	124	156	188	220	252	284	316	348	380	412	444	476	508
I	029	061	093	125	157	189	221	253	285	317	349	381	413	445	477	509
	030	062	094	126	158	190	222	254	286	318	350	382	414	446	478	510
	031	063	095	127	159	191	223	255	287	319	351	383	415	447	479	511

V J P Z Y A X N K S U Q G

512	544	576	608	640	672	704	736	768	800	832	864	896	928	960	992	
513	545	577	609	641	673	705	737	769	801	833	865	897	929	961	993	
514	546	578	610	642	674	706	738	770	802	834	866	898	930	962	994	
515	547	579	611	643	675	707	739	771	803	835	867	899	931	963	995	
516	548	580	612	644	676	708	740	772	804	836	868	900	932	964	996	J
517	549	581	613	645	677	709	741	773	805	837	869	901	933	965	997	B
518	550	582	614	646	678	710	742	774	806	838	870	902	934	966	998	V
519	551	583	615	647	679	711	743	775	807	839	871	903	935	967	999	P
520	552	584	616	648	680	712	744	776	808	840	872	904	936	968		Y
521	553	585	617	649	681	713	745	777	809	841	873	905	937	969		F
522	554	586	618	650	682	714	746	778	810	842	874	906	938	970		C
523	555	587	619	651	683	715	747	779	811	843	875	907	939	971		X
524	556	588	620	652	684	716	748	780	812	844	876	908	940	972		K
525	557	589	621	653	685	717	749	781	813	845	877	909	941	973		N
526	558	590	622	654	686	718	750	782	814	846	878	910	942	974		H
527	559	591	623	655	687	719	751	783	815	847	879	911	943	975		S
528	560	592	624	656	688	720	752	784	816	848	880	912	944	976		U
529	561	593	625	657	689	721	753	785	817	849	881	913	945	977		Q
530	562	594	626	658	690	722	754	786	818	850	882	914	946	978		E
531	563	595	627	659	691	723	755	787	819	851	883	915	947	979		D
532	564	596	628	660	692	724	756	788	820	852	884	916	948	980		L
533	565	597	629	661	693	725	757	789	821	853	885	917	949	981		W
534	566	598	630	662	694	726	758	790	822	854	886	918	950	982		O
535	567	599	631	663	695	727	759	791	823	855	887	919	951	983		G
536	568	600	632	664	696	728	760	792	824	856	888	920	952	984		A
537	569	601	633	665	697	729	761	793	825	857	889	921	953	985		Z
538	570	602	634	666	698	730	762	794	826	858	890	922	954	986		T
539	571	603	635	667	699	731	763	795	827	859	891	923	955	987		R
540	572	604	636	668	700	732	764	796	828	860	892	924	956	988		M
541	573	605	637	669	701	733	765	797	829	861	893	925	957	989		I
542	574	606	638	670	702	734	766	798	830	862	894	926	958	990		
543	575	607	639	671	703	735	767	799	831	863	895	927	959	991		

Le W du deuxième alphabet est utilisé pour compléter le dernier bigramme quand le nombre des lettres à cryptographier est impair.

Au lieu d'employer les bigrammes normaux, nous aurions pu faire usage des bigrammes fractionnés :

r	e	p	u	b	l	i	q	u	e
f	r	a	n	c	a	i	s	e	w
379	434	679	752	453	692	349	817	304	210

Pour assurer l'individualité des dépêches cryptographiées dans ce système, on peut se servir des groupements, des reports, des clés variables, des mots alphabétiques et des opérations arithmétiques.

Il semble parfaitement inutile de nous appesantir sur l'application de ces procédés aux systèmes numériques, dont l'emploi télégraphique est peu pratique pour le chiffrement d'un texte clair ; nous y reviendrons si l'accueil fait au présent travail nous amène à traiter des répertoires et des dictionnaires chiffrés. Il est cependant indispensable de dire quelques mots des changements de clé à la volonté de l'expéditeur.

Lorsque le chiffreur juge opportun de changer la clé qu'il a employée au début de sa dépêche, il inscrit simplement la nouvelle au milieu du texte, si le ternaire qui la représente est en dehors du cadre formé par les nombres utilisables avec la première clé ; si, au contraire, le ternaire pris pour nouvelle clé a une signification littérale avec l'ancienne, on augmente le ternaire choisi, suivant le cas, de vingt-cinq ou de huit cents unités ; dans tous les cas, en l'augmentant ou le diminuant de huit cent vingt-cinq unités, on obtiendra un nombre en dehors du tableau usité jusqu'à ce moment. En effet, supposons que les deux bandes alphabétiques commencent par A et se terminent par Z, le bigramme AA ne pourra avoir pour valeur que l'un des quarante-deux nombres inscrits dans le petit rectangle supérieur à gauche du tableau, et le bigramme ZZ un des quarante-deux nombres du petit rectangle inférieur de droite, dont la valeur est celle des premiers augmentée de huit cent vingt-cinq : on voit facilement le rapport des deux autres rectangles avec les premiers.

De cette manière, il est facile d'introduire dans une dépêche un ternaire qui, n'ayant aucune signification, est, par cela même, désigné comme nouvelle clé et indique la position à donner aux bandes alphabétiques pour continuer la traduction.

Bandes numériques. — Lorsqu'on se trouve dépourvu du tableau, dont l'établissement est long et laborieux, on peut se servir de *bandes numériques*, dont l'emploi est un peu plus pénible, mais qui fournissent les mêmes résultats.

On confectionne ces bandes en inscrivant, sur un papier divisé en intervalles égaux et à quelque distance l'une de l'autre, deux progressions arithmétiques de vingt-six termes, dont le premier est zéro dans les deux séries et dont la raison est l'unité pour l'une et trente-deux pour l'autre.

1er	J	B	V	P	Y	F	C	X	K	N	H	S	U	Q	E	D	L	W	O	G	A	Z	T	R	M	I
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
2e	H	D	B	W	L	O	E	I	F	T	R	C	M	V	J	P	Z	Y	A	X	N	K	S	U	Q	G
	000	032	064	096	128	160	192	224	256	288	320	352	384	416	448	480	512	544	576	608	640	672	704	736	768	800

Ces bandes peuvent aussi être disposées verticalement et de manière à glisser l'une près de l'autre, mais alors leur confection serait plus pénible, chacune d'elles devant porter les lettres et les chiffres qu'il s'agit de rapprocher pour en opérer la combinaison.

Ayant ensuite écrit les deux alphabets conventionnels sur des *bandes indépendantes*, on fait coïncider chacun d'eux avec la série qui lui convient et, pour cryptographier, on ajoute au nombre de la première lettre du bigramme le nombre de la deuxième, prise dans l'autre alphabet, et la clé numérique, Exemple :

R = 23	p = 3	b = 1	i = 25	u = 12
e = 192	u = 736	l = 128	q = 768	e = 192
Clé = 100.......	100	100.........	100	100
315	839	229	893	304
Re	*pu*	*bl*	*iq*	*ue*

Cryptogramme identique avec celui que nous avons trouvé en nous servant du tableau numérique.

La traduction se fait par l'opération inverse : on déduit d'abord, de chaque ternaire, la clé numérique, puis cherchant dans les multiples de trente-deux le plus grand nombre contenu dans le ternaire rectifié, on a une des lettres du bigramme ; le résidu donne l'autre. Il importe de faire attention à la place qu'occupe chacune des lettres dans le bigramme. Exemple :

Ternaires :	425 ...	.760. ...	682.....	.829......	210
Clé à déduire :	100......	100......	100......	100.	100
Restes :	325	660... .	582	729..	..110
1er alphabet :	5 = f	20 = a	6 = c	25 = i	14 = e
2e alphabet :	320 = r	640 = n	576 = a	704 = s	096 = w

Bien que la traduction, ainsi faite, soit un peu longue, elle a l'avantage de suppléer à l'absence de tout document.

Damiers bigrammatiques à trois chiffres. — Les damiers bigrammatiques complets peuvent aussi fournir des ternaires numériques pour représenter les bigrammes. Il suffit, pour cela, de remplacer les deux alphabets auxiliaires par deux séries numériques analogues à celles qui ont servi à établir les bandes ci-dessus. Ces séries n'ont chacune que vingt-cinq termes; la première peut être formée de vingt-cinq multiples de 25, choisis entre les nombres 000 et 975; dans ce cas, l'autre série est donnée par la suite des nombres naturels de 0 à 24: le maximum de la première série n'est plus que 600 (nombre minimum possible de cette série) si l'on emploie dans la deuxième le maximum 399.

Ces damiers donnent de vrais bigrammes numériques qui ne ressemblent en rien aux résultats fournis par le tableau ou par les bandes dont nous venons de faire connaître l'emploi. Ils ont seulement l'inconvénient de nécessiter une petite addition dans le chiffrement et, par suite, une soustraction pour la lecture.

Les bigrammes obtenus, représentés par des ternaires numériques, peuvent être fractionnés mais non scindés, à moins d'employer quatre chiffres, au lieu de trois, pour chaque bigramme cryptographié.

Soit, comme exemple, le damier suivant :

	A	B	C	D	E	000	025	050	075	100	
	F	G	H	I	J	125	150	175	200	225	
1	K	L	M	N	O	250	275	300	325	350	2
	P	Q	R	S	T	375	400	425	450	475	
	U	V	X	Y	Z	500	525	550	575	600	
	0	1	2	3	4	U	P	K	F	A	
	5	6	7	8	9	V	Q	L	G	B	
4	10	11	12	13	14	X	R	M	H	C	3
	15	16	17	18	19	Y	S	N	I	D	
	20	21	22	23	24	Z	T	O	J	E	

Pour cryptographier, opérer comme il est dit à la page 77 : chercher le nombre qui se trouve dans le quartier numéro 2, à l'intersection de la rangée contenant la première lettre du bigramme, lue dans le quartier numéro 1, et de la colonne renfermant la deuxième lettre, lue dans le quartier numéro 3; chercher ensuite, dans le quatrième quartier, le nombre appartenant à la

colonne de la première lettre et à la rangée de la deuxième ; le total de ces deux nombres sera le ternaire numérique correspondant au bigramme.

Exemple :	Vi	ve	la	Fr	an	ce
	575	600	350	150	050	100
	16	21	1	10	15	22
Cryptogramme :	591	621	351	160	065	122

Pour traduire, chercher le plus grand multiple de vingt-cinq contenu dans le ternaire ; ce multiple et son résidu forment les extrémités d'une des diagonales d'un rectangle, dont l'autre diagonale est terminée par les lettres du bigramme correspondant, la première lettre appartenant, sauf convention contraire, au premier quartier et la deuxième lettre au troisième quartier.

Nous arrêterons ici l'étude des cryptogrammes numériques, le nombre des chiffres à employer, un et demi par lettre, rendant peu pratique leur emploi pour la correspondance télégraphique, défaut qui entache, mais à un moindre degré, les cryptogrammes littéraux. Nous y reviendrons, si nous entreprenons l'étude des répertoires, où ces systèmes seront d'une grande utilité.

CINQUIÈME PARTIE

MÉTHODES DIVERSES

Autochiffrement. — Plusieurs cryptologues, notamment Vigenère et MM. Josse et de Viaris, ont exposé des méthodes dans lesquelles les lettres claires ou chiffrées servent de clés pour le chiffrement des lettres suivantes.

Systèmes de Vigenère et G. Selenus. — Ces systèmes dits, à tort, par polygrammes, consistent à chiffrer une ou deux lettres avec des alphabets monolittéraux *fixes*, c'est-à-dire sans variation de clé et à cryptographier la dernière lettre de chaque groupe, en prenant pour clé la lettre claire précédente. On pourrait, sans aucun inconvénient, prendre pour clé le chiffre de cette lettre, ce qui augmenterait, mais dans une faible proportion, les garanties de secret.

Système autoclave. — M. de Viaris a ainsi dénommé le système suivant, qu'il a imaginé pour éviter « toute répétition d'alphabets et, par suite, de polygrammes semblables dans le texte cryptographié ».

Ce système consiste à cryptographier, avec la clé convenue, les premières lettres du texte clair, qui servent ensuite de clés pour les suivantes, lesquelles deviendront clés à leur tour, etc.

Ici encore, au lieu de prendre pour clés les lettres successives du texte clair, il y aurait un petit avantage à se servir de leurs chiffres.

Système Delauney perfectionné. — « Ce système, dit M. Valério, décrit déjà dans l'ouvrage de Blaise de Vigenère, a

été, en 1884, inventé par le capitaine d'artillerie Delauney et perfectionné par M. Josse .»

Soit l'alphabet numérique conventionnel :

Y	M	B	O	Z	A	C	P	S	D	Q	E	F	T	N	G	U	R	H	V	I	J	X	L	K
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24

Chiffrons : *Partez demain matin.*

I	p	a	r	t	e	z	d	e	m	a	i	n	m	a	t	i	n
II	7	5	17	13	11	4	9	11	1	5	20	14	1	5	13	20	14
III	7	12	4	17	3	7	16	2	3	8	3	17	18	23	11	6	20
IV	P	F	Z	R	O	P	U	B	O	S	O	R	H	L	E	C	I

La ligne I contient le texte clair ; la ligne II, la valeur numérique de chaque lettre d'après l'alphabet conventionnel.

La ligne III est formée des totaux successifs des valeurs numériques de toutes les lettres chiffrées. Lorsque l'un de ces totaux dépasse vingt-cinq, on en retranche ce nombre, l'alphabet ne possédant que vingt-cinq lettres. On a ainsi : $12=7+5$, $4=12+17-25$, $17=4+13$, $3=17+11-25$, etc.

La ligne IV contient la traduction en lettres des nombres III, d'après l'alphabet conventionnel.

Au lieu d'employer l'alphabet numérique et de faire des calculs qui, malgré leur simplicité ne laissent pas d'être fastidieux et de présenter des chances d'erreurs, on peut disposer l'alphabet conventionnel : Y M B O Z A C P... etc., en chiffre carré et chiffrer chaque lettre claire au moyen du sous-alphabet désigné par la lettre précédente du chiffre.

L'emploi des bandes alphabétiques est encore plus simple et permet d'obtenir, si l'on veut, des cryptogrammes correspondant à ceux que fournirait un second alphabet numérique servant à transformer en lettres les nombres de la ligne III.

M. Valério fait remarquer que le « système d'autochiffrement » présente un grave inconvénient : si une erreur se produit, elle » se répercute sur tous les chiffres suivants de la dépêche ».

On peut obvier à cet inconvénient par l'emploi des groupements, fixes ou variables, convenus d'avance ou laissés à la volonté de l'expéditeur. Les erreurs sont ainsi localisées, et, par conséquent, plus faciles à reconnaitre et à rectifier. Il est bon de se servir aussi d'une lettre signal pour chiffrer la première lettre de chaque groupe et qui peut, à la rigueur, en se chiffrant elle-même, à intervalles réguliers ou irréguliers, fragmenter une longue dépêche en une série de petites.

En prenant pour clé d'une lettre à cryptographier la lettre claire précédente, au lieu de son chiffre, on empêche également

l'erreur de se propager, puisqu'elle ne peut porter que sur deux lettres au plus et les garanties de secret restent à peu près les mêmes.

Fragmentation incomplète des lettres et transformation des nombres en chiffres différents. — Par l'adjonction d'un alphabet conjugué, la méthode exposée page 118 et suivantes donne de curieux résultats qu'il est bon de faire connaître. Entre autres bizarreries, les cryptogrammes de ce système ont parfois moins, souvent plus de lettres que le texte clair et très rarement le même nombre.

Soient les deux alphabets :

Alphabet n° 1.

	0	1	2	3	4	5	6	7	8	9
»	—	<	S	T	E	N	A	U	I	R
0	+	D	M	F	H	Y	W	C	Q	J
1	=	K	P	B	L	G	O	Z	V	X

Alphabet n° 2.

	0	1	2	3	4	5	6	7	8	9
»	S	E	R	A	<	—	L	O	I	N
4	B	F	J	P	U	+	Y	D	K	T
5	Z	H	V	G	X	=	Q	C	M	W

La première ligne horizontale renferme les chiffres des unités et la première colonne verticale les chiffres de dizaines.

On chiffre avec le premier alphabet comme il est dit à la page 119, puis on traduit les nombres en lettres avec le second alphabet. Quand un chiffre isolé reste à la fin de la dépêche, si c'est un des chiffres de dizaines du deuxième alphabet, ce chiffre n'ayant pas de valeur littérale, on le fait suivre de l'un des chiffres sans valeur du premier alphabet et l'on traduit alors sans difficulté.

Exemples : Cryptographier le mot *Paris*.

1er alphabet : *P a r i s*
12 6 9 8 2
2e alphabet : ER L N I R

Traduire : S A N L Z O B 2e alphabet.
03 9 6 5 07 40
F r a n c e 1er alphabet.

Le 0, qui a été introduit par la nécessité d'adjoindre un chiffre d'unités au 4 final, n'a d'autre signification que celle de *point final*. Il en eût été de même du chiffre 1.

Pour la *transformation d'une série numérique en une autre série*, il est indispensable d'assigner un caractère spécial aux chiffres de dizaines lorsque, *terminant un nombre, ils se trouvent isolés*. Ces caractères, n'étant pas transmis, peuvent affecter telle forme que l'on veut : lettres grecques, signes arithmétiques, etc.

Le travail de transformation consiste à traduire les nombres donnés en lettres d'après un alphabet convenu, puis à convertir, d'après un second alphabet conventionnel, les lettres en chiffres.

Exemple :	1er alphabet :	3	$\overline{14}$	$\overline{15}$	9
		$\underline{\text{T}}$	L	$\underline{\text{G}}$	R
	2e alphabet :	49	6	53	2

d'où : 314159 = 496532.

Soit encore :	$\underline{19}$	$\underline{00}$		$\underline{18}$	81	
	$\underline{\text{X}}$	$\underline{+}$	1900 = 5445	$\underline{\text{V}}$	I<	1881 = 5284
	54	45		52	84	

Cette méthode, sur laquelle nous ne nous étendrons pas, pourra trouver son application dans l'emploi des répertoires et dictionnaires chiffrés.

Bandes alphabétiques et numériques. — Au lieu de bandes simplement littérales, les bandes alphabétiques élargies peuvent porter en même temps les lettres et leurs valeurs numériques, ce qui permet d'y appliquer une clé à l'aide des obturateurs déjà étudiés, ou des formules cryptographiques, et d'obtenir, non seulement tous les résultats que fournissent les bandes simples, mais encore de transformer les chiffres en lettres et réciproquement.

SIXIÈME PARTIE

APPAREILS CRYPTOGRAPHIQUES

Les *appareils cryptographiques,* connus encore sous le nom de *cryptographes,* sont fort nombreux.

La *première classe* renferme les appareils de *transposition,* tels que la *scytale* des Lacédémoniens, qui transpose et fractionne les lettres, l'*appareil* de Rondepierre, le *taquin* de M. le capitaine Delauney, les *tablettes* de M. de Viaris, les *jeux de cartes,* les *grilles,* etc.

De l'étude, bien incomplète encore, que nous avons faite des grilles, il doit résulter, pour le lecteur sans parti pris, que ce petit appareil est appelé à rendre d'immenses services en cryptographie. Son emploi est sûr et facile ; on ne peut plus lui reprocher que l'inconvénient, fort grave, à la vérité, d'exiger un secret absolu, sa conservation paraissant indispensable, vu le temps et le travail nécessaires pour confectionner une grille d'après les indications convenues.

En réalité, ce défaut n'existe pas et nous nous proposons de faire construire des *grilles cryptographiques* qui pourront, sans le moindre inconvénient, être mises dans toutes les mains et même livrées au commerce.

La *seconde classe* renferme les appareils *de chiffrement proprement dit.*

Ici nous retrouvons encore la *grille ;* puis viennent les cryptographes de Porta, Grivel, Wheatstone, Pantin-Richard, Kerck-

hoffs, Vinay et Gaussin, Silas, Mouilleron, Kronenberg, Pasanisi, Köhl, Lemarchand, Hennet, de Viaris, Bossuat, Bazeries, Hermann, Ducros, etc.

Tous ces appareils, autant que nous pouvons en juger par les descriptions publiées, sont des instruments, qui ne font que réaliser mécaniquement ou plutôt faciliter l'opération du chiffrement, mais aucun ne sort des principes que nous avons exposés et ne donne lieu à des combinaisons nouvelles.

De tous ces appareils, très peu sont réellement portatifs et d'un emploi facile pour une armée en campagne ; en outre, en dépit de mécanismes ingénieux qui permettent d'imprimer tant les dépêches que leur traduction, tel que le cryptographe de M. de Viaris, ils ne sont, pour la plupart que des applications du chiffre carré de Vigenère et, par suite, les dépêches, ainsi cryptographiées, présentent tous les inconvénients inhérents à cette méthode.

Deux de ces appareils cependant sont basés sur des systèmes différents et il convient de les mentionner d'une manière spéciale. Ce sont le *cryptographe cylindrique* de M. le commandant Bazeries et le *scotographe* de M. Ducros, colonel d'artillerie de l'armée italienne et directeur de la fabrique d'armes à Torre Annunziata.

Le **cryptographe Bazeries** consiste essentiellement en un cylindre sur lequel on enfile vingt rondelles portant chacune les vingt-cinq lettres de l'alphabet, disposées dans un ordre différent.

Toutes les rondelles sont, en outre, marquées en côté d'un numéro d'ordre servant à les classer selon les indications de la clé.

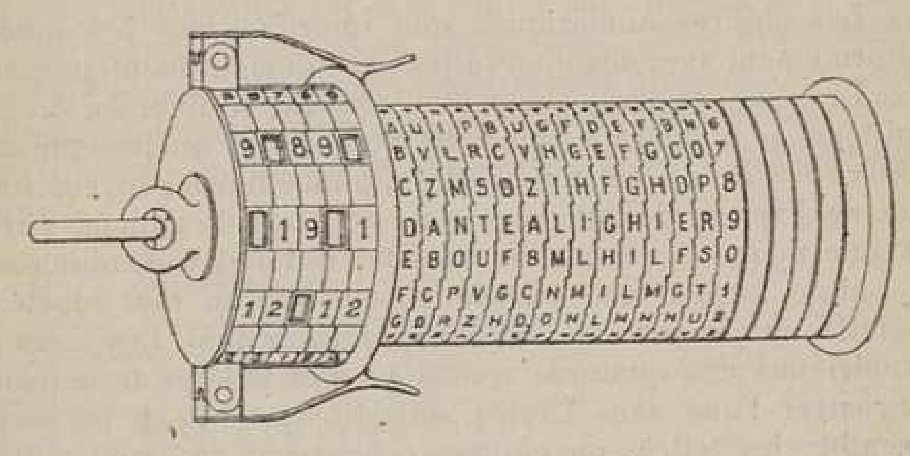
L'emploi du cryptographe cylindrique est le même que celui des bandes polyalphabétiques, que nous avons précédemment étudiées (voir pages 51 et suivantes).

Bien que sa forme se rapproche beaucoup de celle du cryptographe cylindrique, le *scotographe* (du grec *scotos*, obscurité, ténèbres) en diffère entièrement, tant par sa disposition que par son principe.

M. L. Gioppi, le savant auteur de la Crittografia (1), a bien voulu me donner communication de l'article qu'il a publié, en 1900, dans la *Rivista Militare Italiana*, sur le scotographe et me transmettre l'autorisation de M. le colonel Ducros de reproduire la description de son ingénieux instrument. Je tiens à remercier, ici, ces deux éminents cryptologues de la courtoisie dont ils ont fait preuve à mon égard.

(1) Milano, Hoepli, édit., 1897.

Scotographe Ducros. — Nous extrayons la description du scotographe de l'article de M. L. Gioppi, à qui nous empruntons, en outre, la figure de l'appareil.



« Le *scotographe* se compose d'une sorte d'étui cylindrique en
» métal, de quatorze rondelles dentelées et d'un collier mobile.
» Treize des quatorze rondelles portent imprimées les lettres de
» l'alphabet et, sur la dernière, sont gravés des chiffres numé-
» riques. Le collier mobile est composé de cinq anneaux dentelés,
» où sont imprimés des chiffres numériques et dont le premier
» à gauche dans la figure, est muni de deux fermoirs à ressort
» denté. L'étui a deux parties qui s'unissent par un pas de vis ;
» la plus grande, qui forme le corps de l'étui et porte les ron-
» delles, a un bourrelet contre lequel ces mêmes rondelles sont
» légèrement serrées par l'autre partie de l'étui servant de
» couvercle.

» Dépourvu du collier mobile, le scotographe a une grande analogie avec les cadenas dits *à combinaisons*. L'intérieur de l'étui peut être utilisé pour serrer papier, crayon, gomme, etc.

» Chacune des treize rondelles alphabétiques porte imprimé, sur sa surface cylindrique, un alphabet dont les lettres sont distribuées à intervalles parfaitement égaux, et dont la séquence, identique pour les treize rondelles, est la suite naturelle de l'alphabet classique. Ces lettres, au nombre de vingt, sont les lettres indispensables de l'alphabet italien : J, K, Q, W, X et Y manquent.

» On remplace Q par C et on écrit CUELLO pour QUELLO, etc.

» La quatorzième rondelle porte gravée, à intervalles parfaitement égaux, une double numération des chiffres 0 à 9.

» Le collier d'anneaux s'enfile sur la superficie cylindrique des rondelles, enfilées elles-mêmes sur le corps de l'étui.

» Il est constitué par cinq anneaux dentelés, dont la largeur est égale à celle des rondelles. La superficie cylindrique externe de chaque anneau numérique est divisée en vingt intervalles sur lesquels, alternant avec des espaces vides ou muets, sont

imprimés les chiffres 1 à 9. A la place du zéro, c'est-à-dire entre 1 et 9, existe une petite fenêtre rectangulaire.

» Les cinq anneaux du collier sont serrés ensemble à l'aide des fermoirs dentés.

» Les chiffres numériques sont imprimés sur les anneaux uniformément avec des intervalles parfaitement identiques entre eux. Les cinq anneaux du collier peuvent se fixer en diverses positions, de manière à former un nombre-clé quelconque entre 00000 et 99999. Les treize rondelles alphabétiques peuvent, à leur tour, se disposer de telle sorte que, en lisant de gauche à droite sur une même ligne, comme dans les cadenas à combinaisons, on puisse former une phrase choisie ou un mot répété. La rondelle numérique est enfilée en dernier lieu. Les faces non cylindriques des quatorze rondelles sont taillées de manière à s'encastrer l'une dans l'autre, de telle sorte qu'en les serrant ensemble les lettres ou chiffres contigus se trouvent toujours alignés sur une même droite.

» Supposons le *scotographe* monté, c'est-à-dire les rondelles enfilées, le couvercle serré et le collier en place.

» Si l'on fait alors glisser le collier sur les rondelles et que, regardant par une des petites fenêtres rectangulaires, on aperçoit en dessous une lettre quelconque, on reconnait promptement que toutes les autres fenêtres découvrent, chacune de son côté, une lettre des rondelles inférieures.

» Cette coïncidence, voulue, est due à l'identité des intervalles existant entre les lettres de toutes les rondelles et entre les chiffres de tous les anneaux du collier. »

Nous ne croyons pas utile de reproduire les indications données par M. L. Gioppi sur l'établissement des deux clés, l'une littérale, l'autre numérique, non plus que sur le moyen de déduire la seconde de la première à l'aide de la quatorzième rondelle, notre but étant seulement de faire connaître un ingénieux instrument qui peut se définir : *l'application d'une grille au chiffre de Vigenère.*

On cryptographie à l'aide du scotographe d'après la règle suivante :

« Pour chiffrer une dépêche, il faut encadrer les lettres claires de cette dépêche, lues l'une après l'autre sur les rondelles de gauche à droite, dans les fenêtres successives du collier et prendre, chaque fois, pour la lettre correspondante du texte obscur, celle qui apparait à la fenêtre suivante du collier. »

Pour la traduction, il faut faire l'opération inverse, c'est-à-dire « encadrer successivement dans les fenêtres du collier, en commençant par la seconde, chaque lettre du texte obscur et prendre pour lettre correspondante du texte clair celle qui, à chaque position, apparait à la fenêtre précédente du collier. »

Cet exposé suffisant pour qu'on puisse se rendre un compte exact du scotographe Ducros, nous allons maintenant étudier le fonctionnement des deux clés.

Dans la figure qui précède, l'instrument est monté sur la clé littérale DANTEALIGHIER et le collier sur l'un des nombres : 01901, 12012, 23123, 34234, 45345, 56456, 67567, 78678, 89789, 90890, qui, par suite de la disposition uniforme des anneaux sont tous solidaires et déterminent une unique position des fenêtres.

Développons les alphabets des rondelles et les chiffres des anneaux :

Alphabet n° 1.

N	I	Z	E	O	I	U	T	R	S	T	O	C
O	L	A	F	P	L	V	U	S	T	U	P	D
P	M	B	G	R	M	Z	V	T	U	V	R	E
R	N	C	H	S	N	A	Z	U	V	Z	S	F
S	O	D	I	T	O	B	A	V	Z	A	T	G
T	P	E	L	U	P	C	B	Z	A	B	U	H
U	R	F	M	V	R	D	C	A	B	C	V	I
V	S	G	N	Z	S	E	D	B	C	D	Z	L
Z	T	H	O	A	T	F	E	C	D	E	A	M
A	U	I	P	B	U	G	F	D	E	F	B	N
B	V	L	R	C	V	H	G	E	F	G	C	O
C	Z	M	S	D	Z	I	H	F	G	H	D	P
D	A	N	T	E	A	L	I	G	H	I	E	R
E	B	O	U	F	B	M	L	H	I	L	F	S
F	C	P	V	G	C	N	M	I	L	M	G	T
G	D	R	Z	H	D	O	N	L	M	N	H	U
H	E	S	A	I	E	P	O	M	N	O	I	V
I	F	T	B	L	F	R	P	N	O	P	L	Z
L	G	U	C	M	G	S	R	O	P	R	M	A
M	H	V	D	N	H	T	S	P	R	S	N	B
N	I	Z	E	O	I	U	T	R	S	T	O	C
O	L	A	F	P	L	V	U	S	T	U	P	D
P	M	B	G	R	M	Z	V	T	U	V	R	E

Alphabet n° 2.

4	5	3	4	5
5	6	4	5	6
6	7	5	6	7
7	8	6	7	8
8	9	7	8	9
9		8	9	
	1	9		1
1	2		1	2
2	3	1	2	3
3	4	2	3	4
4	5	3	4	5
5	6	4	5	6

Les lecteurs désireux de se rendre exactement compte du jeu de l'appareil pourront, à défaut de scotographe, se servir du tableau ci-dessus en faisant usage d'une grille dont les fenêtres seront disposées comme les cases ombrées de la figure 2. — Pour faciliter le report de la grille d'un côté à l'autre du tableau littéral, il sera bon de reproduire, à la droite, la première colonne de ce tableau.

Chiffrons, pour exemple : *Nous vous attendons à Rome.*

Posons la grille de manière que sa première fenêtre encadre le *n* du premier alphabet et prenons pour lettre chiffre le G, qui apparaît dans la deuxième fenêtre ; faisant ensuite glisser verticalement la grille, nous encadrons l'*o* du deuxième alphabet dans cette même deuxième fenêtre, son chiffre H est lu dans la troisième fenêtre, qu'on fait glisser verticalement pour découvrir l'*u* du troisième alphabet, dont le chiffre A, se montre à la quatrième fenêtre, etc.

N o u s v o u s a t t e n d o n s à R o m e
G H A B T Z A N Z Z M V V V F R H R B P G L

Une seule bande alphabétique nous aurait donné le même cryptogramme avec la clé numérique système Gronsfeld) : 15. 15 . 3 . 6 . 18 7 . 3 . 16 19 . 3 . 14 14..... Mais, par suite de l'emploi de treize alphabets et de cinq ouvertures à la grille, le nombre des termes de la clé s'élève à 13 × 5 = 65, ce qui la rend plus que difficile à retenir de mémoire, mais elle peut aisément se déduire des clés normales du scotographe.

Dans l'exemple qu'il donne de l'emploi de cet instrument, M. L. Gioppi cryptographie : *Situazione molto critica. Occorrono rinforzi*, avec la double clé : *Chi s'aiuta Dio l* 4 2 1 0 9

Nous allons montrer qu'on obtient exactement le même résultat que lui avec un *obturateur en escalier double*. (Voir pages 32 et suivantes).

Si nous transformons la clé littérale en clé de Gronsfeld nous aurons :

c h i s a i u t a d i o l
2.7.8 15.0 8 17 16 0.3 8.12.9

Mais chaque lettre chiffre se lisant sur la bande qui suit celle où on a lu la lettre claire, la clé *réelle* est formée par les différences des nombres de la clé *convenue ;* on aura donc, en répétant à droite le premier nombre de gauche, les clés :

	c	*h*	*i*	*s*	*a*	*i*	*u*	*t*	*a*	*d*	*i*	*o*	*l*	*c*
convenue :	2	7	8	15	0	8	17	16	0	3	8	12	9	2
réelle :	5	1	7	5	8	9	19	4	3	5	4	17	13.	

Cette suite numérique fournit tous les éléments nécessaires pour découper le grand obturateur ; le petit sera construit d'après les indications de la clé numérique *apparente* : 4 2 1 0 9.

La moitié des cases des anneaux du collier étant dépourvues de chiffres, il faut doubler ceux de la clé pour les mettre en concordance avec les cases des rondelles littérales, la *vraie* clé numérique convenue est donc : 8 . 4 . 2 . 0 . 18. Ces nombres nous feront connaître la position relative des fenêtres. En retranchant chacun d'eux de 20, nombre total des cases, pleines ou vides, de chaque anneau, on aura : 12 . 16 . 18 . 0 . 2 . 12 et les différences de ces nombres : 4 . 2 . 2 . 2 . 10 formeront la clé *réelle*. Ce calcul peut être simplifié, car 20—8, diminué de 20 — 4 = — 8 + 4 et (20—4) — (20—2) = —4+2..., etc. d'où il suit que, pour avoir la clé *réelle*, il suffit de doubler chacun des chiffres de la clé *apparente*, puis de chercher leurs différences, en retranchant chaque nombre de celui qui est à sa gauche :

Clé convenue vraie : 8.4.2.0.18 . 8
Clé réelle : 4.2.2.2 . 10

Cette dernière suite de nombres servira à la confection du petit obturateur destiné à glisser sur le grand pour donner la clé complète, dont voici les premiers termes :

Clé numérique :	4	2	2	2	10.	4	2	2	2	10.	4	2	2	2	10.	4	2	2	2	10.	...
Clé littérale :	5	1	7	5	8	9	19	4	3	5	4	17	13.	5	1	7	5	8	9	19	...
Clé complète :	9	3	9	7	18	13	1	6	5	15	8	19	15	7	11	11	7	10	11	9	...

Cette clé, appliquée au texte clair donné plus haut, fournira le cryptogramme obtenu par M. L. Gioppi avec le scotographe :

s i t u a z i o n e m o l t o c r i t i ....
E N F E V O L V T Z V N E D D P B V H U ....

Cette méthode s'applique aussi bien aux alphabets intervertis qu'à l'alphabet normal, complet ou incomplet.

SEPTIÈME PARTIE

CRYPTOGRAPHIE MILITAIRE

Une dépêche, *isolée et courte*, convenablement composée, peut souvent défier toutes les recherches des déchiffreurs et rester inviolable ; faut-il en conclure que toutes les dépêches cryptographiées d'après le même système seront, elles aussi, indéchiffrables ? Ce serait une erreur de le croire ; dans la plupart des cas, l'inviolabilité est due à la brièveté de la dépêche ; que cette brièveté disparaisse ou que l'*ennemi* parvienne à collectionner un certain nombre de cryptogrammes courts mais chiffrés avec la même clé et il lui devient souvent facile de déchiffrer les correspondances, ce qui peut avoir les conséquences les plus funestes, surtout au point de vue militaire.

Il est donc indispensable, pour le service de l'armée, que les systèmes employés remplissent certaines conditions particulières que M. Kerckhoffs a résumées comme suit : (1)

« 1° Le système doit être matériellement, sinon mathématiquement, indéchiffrable ;

» 2° Il faut qu'il n'exige pas le secret, et qu'il puisse sans inconvénient tomber entre les mains de l'ennemi ;

» 3° La clé doit pouvoir en être communiquée et retenue sans le secours de notes écrites, et être changée ou modifiée au gré des correspondants ;

» 4° Il faut qu'il soit applicable à la correspondance télégraphique ;

» 5° Il faut qu'il soit portatif et que son maniement ou son fonctionnement n'exige pas le concours de plusieurs personnes.

(1) *Cryptographie militaire*, page 8.

« 6° Il est nécessaire, vu les circonstances qui en commandent » l'application, que le système soit d'un usage facile, ne demandant ni tension d'esprit, ni la connaissance d'une longue série » de règles à observer. »

Enfin, après examen des différents systèmes, M. Kerckhoffs (1) conclut que la solution du problème doit « être cherchée dans » l'application de quelque appareil mécanique, basé sur le principe d'interversion, c'est-à-dire dans l'emploi d'un *cryptographe* ».

M. le commandant Josse (2), loin d'admettre cette conclusion, ajoute une nouvelle condition ainsi conçue :

« 7° Il faut que le système ne comporte pas l'emploi d'un livre » ou d'un appareil ; » et il formule le principe suivant :

« *La cryptographie militaire, proprement dite, doit employer* » *un système n'exigeant qu'un crayon et du papier.* »

De notre côté, dans un précédent travail (3), nous avons cru devoir ajouter aux conditions précédentes :

« 8° Le rapprochement d'un cryptogramme et de sa traduction » ne doit jamais permettre de découvrir la clé ni, par suite, de » déchiffrer la partie non traduite d'une dépêche dont on possède » le reste en clair. »

Une étude sérieuse des principes cryptographiques conduit à reconnaître que tous les systèmes, même les plus simples, peuvent satisfaire aux huit conditions ci-dessus énoncées, pourvu qu'on en fasse un usage raisonné au lieu de s'en tenir, comme on le fait trop généralement à la stricte application d'une méthode qui, si sûre qu'elle soit, finira par être reconnue et pénétrée lorsque les déchiffreurs ennemis seront parvenus à collectionner une quantité suffisante de cryptogrammes, surtout s'ils peuvent y joindre la traduction de quelques-uns d'entre eux.

Dans un service régulier, il convient donc de faire choix de *plusieurs* systèmes donnant des cryptogrammes de *même apparence*. Ces systèmes, employés chacun pendant un temps plus ou moins long, ne laisseraient pas de dérouter les déchiffreurs et, par conséquent, contribueraient à assurer le secret de la correspondance. Les ordres de changement de système seraient transmis en même temps que le mot d'ordre servant de clé générale.

Un chiffreur ne doit jamais perdre de vue que la difficulté du déchiffrement est en raison inverse de la longueur d'un cryptogramme, d'où il résulte, pour les systèmes alphabétiques surtout, qu'il convient de faire usage de clés multiples (voir pages 110 et

(1) *Cryptographie militaire*, page 60.
(2) *Cryptographie*, page 99.
(3) *Cryptographie nouvelle*, page 54.

111) afin de transformer les longs cryptogrammes en une série de courtes dépêches et de prendre pour règle absolue que :

Chaque dépêche doit être cryptographiée avec une clé individuelle, la même clé ne devant jamais servir à chiffrer plusieurs dépêches.

Il ne doit pas non plus oublier ce principe essentiel de toute bonne méthode : *Le traducteur ne doit jamais être astreint à aucune espèce de tâtonnement, les opérations à effectuer devant être parfaitement définies par les conventions.*

Quant aux livres et appareils, dont l'emploi peut être de la plus grande utilité dans certains cas (quartier général, places fortes, etc.), ils doivent être absolument exclus du service de campagne s'ils sont, et c'est là leur principal mérite, indispensables pour l'échange des correspondances chiffrées.

Ceci peut sembler paradoxal, mais, sans nous arrêter au cas où l'appareil, *en état de fonctionner,* tombe entre les mains de l'ennemi, n'est-il pas évident que si, par fortune de guerre, un officier se trouve démuni de l'appareil qui seul peut lui permettre de traduire les cryptogrammes qu'il reçoit, il lui sera impossible de se conformer aux ordres qui lui sont transmis.

Rédaction des cryptogrammes militaires. — Nous empruntons les lignes qui suivent au savant ouvrage de M. le commandant Josse (1) :

« Un cryptogramme militaire doit être toujours *très concis,*
» tout en restant *très clair :* ce sont là deux conditions indispen-
» sables, mais qu'il n'est pas toujours facile de concilier.

» Souvent, dans le but d'abréger le travail, on ne chiffre
» qu'une partie d'un texte en laissant les autres en clair. Le
» choix des parties qu'il y a lieu de chiffrer est de la plus haute
» importance : si ce choix est maladroit, on risque fort de livrer
» la clé de son système. Il n'y a point de règles précises à donner
» à cet égard, d'autant plus que le choix des parties à chiffrer
» ou à laisser en clair dépend le plus souvent de circonstances
» diverses qu'il est impossible de préciser à l'avance ; dans tous
» les cas, il est absolument nécessaire que l'officier chargé de
» chiffrer un texte possède une pratique suffisante du *chiffre*
» qu'il doit employer.

» Lorsqu'il s'agit de transmissions télégraphiques, il est indis-
» pensable de faire usage de signes conventionnels de *ponctua-*
» *tion :* la dépêche y gagnera considérablement en clarté lors-
» qu'elle sera soumise à la traduction.

» Il existe enfin certaines règles, applicables à toutes les

(1) *Cryptographie,* page 102.

» communications télégraphiques, mais plus particulièrement
» encore lorsqu'il s'agit de cryptogrammes :

» 1° Lorsqu'il n'y a pas de bureau ou de poste télégraphique
» dans la localité même où l'on écrit la dépêche, il faut toujours
» commencer le texte chiffré par l'indication en *clair* (à moins
» qu'il en soit ordonné autrement) du *lieu* et de la *date*. Dans
» certains cas importants il faudra même y ajouter l'indication
» de l'*heure* ;

» 2° Ne jamais expédier (sauf le cas de nécessité absolue) un
» texte chiffré, sans l'avoir déchiffré soi-même, ou mieux encore,
» fait traduire par un autre officier : on s'apercevra ainsi des
» erreurs qui auront pu être commises pendant l'opération du
» chiffrement ;

» 3° Les textes remis aux télégraphistes doivent être écrits
» très lisiblement et avec le plus grand soin : il faut séparer
» nettement les groupes de lettres ou de chiffres ;

» 4° Les papiers qui ont servi aux opérations de chiffrement
» ou de traduction doivent toujours être *brûlés*.

» Ces règles, qui ont pour elles la sanction de la pratique,
» doivent être rigoureusement observées dans l'intérêt de la
» sécurité des correspondances cryptographiées.

HUITIÈME PARTIE

DÉCHIFFREMENT

La *cryptophotie*, ou l'art de déchiffrer les écritures secrètes, dès longtemps pratiquée par quelques personnes, parmi lesquelles nous ne citerons que Rossignol de Juvisy et le géomètre Viète, père de l'algèbre moderne, était peu connue et peu répandue, tant à cause du danger couru par les déchiffreurs, que des difficultés de toute sorte inhérentes au déchiffrement. M. le commandant Josse consacre près d'une page à la simple énumération des *qualités naturelles ou acquises, que doit posséder un déchiffreur* (*Cryptographie*, page 11).

Ce n'est que depuis une quarantaine et surtout une vingtaine d'années que la cryptophotie s'est développée et est sortie de l'art pur ou de la divination pour prendre une allure plus scientifique, à la suite des travaux de Vesin de Romanini, Kasiski. Fleissner von Vostrowitz, Kerckhoffs, Bazeries et de Viaris, mais le principal traité de déchiffrement, on pourrait presque dire le seul. est dû à M. le capitaine Valério, qui a publié en 1893 un important et laborieux travail, où toutes les méthodes en usage alors sont étudiées, disséquées pour ainsi dire, de manière à mettre en évidence leurs points faibles et à en déduire le moyen d'atteindre le secret qu'elles ont pour mission de dissimuler.

Nous n'entreprendrons ni de résumer, ni d'analyser ce chef-

d'œuvre d'induction et de patience, ce serait œuvre vaine ; tous les lecteurs que l'art de déchiffrer intéresse devront recourir au traité que son savant auteur intitule modestement un essai.

Mais, comme il est absolument nécessaire à tout chiffreur de connaitre les *principes généraux* du déchiffrement, nous allons en donner quelques notions, indispensables pour permettre de bien apprécier la valeur relative de chacun des systèmes que nous avons exposés.

Méthodes de transposition. — Le déchiffrement des cryptogrammes fournis par ces méthodes repose principalement sur les particularités de la langue employée que, dans tout ce qui va suivre, nous supposerons être la langue française.

On recherchera surtout les lettres qui s'accompagnent, sinon forcément, du moins presque toujours : *qu*, *ix*. (Voir, à ce sujet, la *Cryptographie* de M. Josse, pages 14 et suivantes, et celle de M. Valério, pages 13 et 61.)

La détermination d'un bigramme entraine, pour les grilles, la connaissance de deux fenêtres, et pour les carrés ou rectangles (méthode des diviseurs), la disposition de deux colonnes ; discutant ensuite la probabilité des lettres voisines, on arrive à déterminer une troisième fenêtre, ou une troisième colonne, suivant le cas, et peu à peu, on parvient à reconstituer le texte clair.

M. Valério (1) a dénommé lettres *indicatrices* celles qui, offrant peu de combinaisons, doivent évidemment être considérées tout d'abord, ce sont : Q, X, F, H, J.

Souvent, bien que éparses, les lettres constitutives laissent apparaitre certains mots, ainsi, dans les dépêches militaires, les expressions : armée, division, officiër, général, ennemi, etc., sautent aux yeux des déchiffreurs un peu exercés.

D'autre part, les lettres *nulles*, préconisées par certains auteurs, augmentent peu la difficulté du déchiffrement : elles se séparent spontanément du texte.

Pour preuve, proposons-nous de déchiffrer la dépêche suivante, que nous trouvons dans le *Dictionnaire Militaire*, page 783:

iouvSrouelzqeooladpMotaltrabemenlnmeMatisnruocieozohgy
bxgicosnczucdomiasemhroenordfcJpemteArcaeotn.

L'examen de ce cryptogramme nous conduit à supposer qu'il a été établi par une méthode de transposition : sur les quatre-vingt-dix-huit lettres qu'il contient, on compte, en effet, quarante voyelles, dont onze E ; or, en français, la proportion de l'E, sur

(1) *Cryptographie*, page 162.

cent lettres, varie, en général, de 14 à 20 et celle des voyelles de 42 à 46.

Si, par ailleurs, nous sommes amenés à supposer qu'on a employé la méthode des carrés, nous diviserons notre cryptogramme en deux parties de quarante-neuf lettres chacune, que nous écrirons sur sept lignes divisées en sept colonnes, comme le montrent les diagrammes ci-dessous :

N° 1.

	1	2	3	4	5	6	7
1	i	o	u	v	S	r	o
2	u	e	l	z	q	e	o
3	o	l	a	d	p	M	o
4	t	a	t	t	r	a	b
5	e	m	e	n	l	n	m
6	e	M	a	t	i	s	n
7	r	u	o	c	i	e	o

N° 2.

	1	2	3	4	5	6	7
1	z	o	h	g	y	b	x
2	g	i	c	o	s	n	c
3	z	u	v	d	o	m	i
4	a	s	e	m	h	r	o
5	e	n	o	r	d	f	v
6	J	p	e	m	t	e	A
7	r	e	a	e	o	t	n

Occupons-nous exclusivement du tableau numéro 1 et cherchons d'abord dans quel sens il doit être lu, en d'autres termes, si le relèvement a été horizontal ou vertical.

Le texte renferme vingt-trois voyelles, soit une moyenne de 3,29 par groupe, rangée ou colonne, de sept lettres.

Les *rangées* contiennent respectivement : 4, 4, 3, 2, 2, 3, 5 voyelles qui donnent, par rapport à la moyenne, 3,29, des écarts, en plus ou en moins, égaux à :

0,71 0,71 0,29 1,29 1,29 0,29 1,71

soit un écart moyen de 0,89.

Les *colonnes* contiennent : 5, 4, 5, 0, 2, 3, 4 voyelles qui donnent des écarts de :

1,71 0,71 1.71 3,29 1,29 0,29 0,71

soit un écart moyen de 1,39, bien plus considérable que le premier.

Nous en concluons que le relèvement a été fait par rangées ou lignes horizontales, la proportion des voyelles étant plus constante.

Il s'agit maintenant de rétablir l'ordre primitif des colonnes de manière que chaque rangée ait un sens, car l'interversion,

tout en changeant l'ordre des lettres, ne parvient pas à mélanger celles qui appartiennent à deux rangées ou à deux colonnes distinctes. — Nous avons vu qu'il n'en est plus ainsi lorsque les *nulles* sont remplacées par des points, supprimés dans le cryptogramme, et que, en outre, le déchiffreur ne possède plus de renseignements sur les dimensions des carrés.

Nous remarquons d'abord, à la deuxième rangée, les lettres U, Q ; le Q étant presque invariablement suivi d'un U, nous admettrons que la colonne 5 doit être suivie de la colonne 1 d'autant plus que les bigrammes formés dans les autres rangées par cette transposition sont tous possibles.

Si cette combinaison ne réussit pas, nous serons conduits à supposer que Q occupe la dernière place de la deuxième rangée et U la première de la septième rangée.

Admettons la combinaison 5-1 et cherchons la colonne suivante. Q U est généralement suivi d'un E ou d'un I, exceptionnellement de A, O, U ; la deuxième rangée renfermant deux E, examinons les trigrammes que donnent les combinaisons de colonnes : 5-1-2 et 5-1-6 ; à la septième rangée, la combinaison 5-1-2 nous fournit *iru*, qui est moins probable que *ire*, adoptons donc la combinaison 5-1-6, qui amène, à la cinquième rangée le trigramme : *len*.

Sachant que nous avons affaire à une dépêche militaire, nous n'hésiterons pas à lire dans cette cinquième rangée, *l'ennemi* et nous disposerons les colonnes dans l'ordre suivant : 5-1-6-4-3, ce qui fournira les pentagrammes :

	5	1	6	4	3	2	7
1re	S	i	r	v	u	o	o
2e	q	u	e	z	l	e	o
3e	p	o	M	d	a	l	o
4e	r	t	a	t	t	a	b
5e	l	e	n	n	e	m	m
6e	i	e	s	t	a	M	n
7e	i	r	e	c	o	u	o

Rapprochons des colonnes déjà placées celles qui restent et nous reconnaissons facilement :

1° Que la deuxième seule donne un sens ;

2° Que la septième n'a aucune valeur et semble n'avoir été introduite que pour dérouter les déchiffreurs.

Les première et troisième rangées paraissent avoir le même but.

Pour nous en assurer, après avoir transposé les *rangées* suivant l'ordre : 5-6-7-4-2 et reconnu qu'elles présentent un sens

suivi, nous nous reporterons au tableau numéro 2, auquel nous ferons subir les mêmes transpositions de colonnes et de rangées, et il viendra :

N° 1.

	5	1	6	4	3	2	7
5	l	e	n	n	e	m	*m*
6	i	e	s	t	a	M	*n*
7	i	r	e	c	o	u	*o*
4	r	t	a	t	t	a	*b*
2	q	u	e	z	l	e	*o*
1	*S*	*i*	*r*	*v*	*u*	*o*	*o*
3	*p*	*o*	*M*	*d*	*a*	*l*	*o*

N° 2.

	5	1	6	4	3	2	7
5	d	e	f	r	o	n	*v*
6	t	J	e	m	e	p	*A*
7	o	r	t	e	a	C	*n*
4	h	a	r	m	e	s	*o*
2	*S*	*g*	*n*	*o*	*e*	*i*	*c*
1	*y*	*z*	*b*	*g*	*h*	*o*	*x*
3	*o*	*z*	*m*	*d*	*v*	*u*	*i*

soit : *L'ennemi est à Mirecourt. Attaquez-le de front. Je me porte à Charmes.* — En plus quarante-quatre lettres nulles.

En discutant les probabilités, on arriverait promptement à déterminer la clé : 5, 1, 6, 7, 4, 3, 2, qui est la même pour les colonnes et les rangées.

Méthodes alphabétiques. — Comme nous le verrons plus loin, le déchiffrement des cryptogrammes chiffrés par des méthodes polyalphabétiques se ramène au déchiffrement de textes cryptographiés à l'aide d'un seul alphabet et d'une clé simple.

Dans ce cas, la forme des lettres change seule; leurs redoublements, leurs sympathies et leurs antipathies, mais surtout leurs fréquences relatives restent les mêmes et, si le texte est assez long, le déchiffreur n'a pas de peine à les reconnaitre sous leurs formes anormales, en un mot, à les démasquer.

Bien que la fréquence des lettres, c'est-à-dire le nombre de fois qu'elles sont répétées dans un texte, varie beaucoup suivant le sujet traité, le style de l'écrivain, etc., nous considérerons comme fréquence normale celle qu'indique M. Valério, soit sur mille lettres :

E	N	A	I	R	S	T	U	O	L	D	C	M	P	V
170	87,3	72,6	68,6	68,6	68,6	67,3	66,6	66	48,6	46	35,3	30,6	28	18

F	B	G	Q	H	X	J	Y	Z	K	W
12,6	9,3	7,3	7,3	5,3	5,3	3,3	3,3	2,7	0	0

Ajoutons à ce tableau les lettres qui se redoublent le plus souvent :

S = 8,0 L = 7,5 E = 6,6 N = 5,6 T = 4,0

Lorsque les mots d'un cryptogramme sont *séparés*, le déchiffrement est généralement facile; alors il repose surtout sur la *conformation* des mots les plus usuels.

Pour exemple, déchiffrons le cryptogramme suivant :

1	2	3	4	5	6	7
JQQJ	JXY	UFWYNJ	UTZW	ZSJ	IJXYNSFYNTS	NSHTSSZJ

Le décompte des lettres donne :

J = 7	N = 4	T = 3	W = 2	X = 2	Q = 2	H = 1
S = 6	Y = 4	Z = 3	F = 2	U = 2	I = 1	

A cause de sa plus grande fréquence, nous admettrons J = *e*; remarquant ensuite que le premier mot est formé d'une lettre redoublée, précédée et suivie d'un *e*, nous en concluons que Q = *l*, *elle* étant le seul mot usuel qui présente cette particularité.

Le deuxième mot, JXY, est un trigramme commençant par un *e*; les mots : *eau*, *ému*, *épi*, *eux*, etc., sont inadmissibles, mais *est* semble tout indiqué. Acceptons-le.

Le cinquième mot, ZSJ, est encore un trigramme et il finit par un *e*. Les seuls trigrammes usuels qui se trouvent dans ce cas sont *que* et *une*. Ici *que* ne convient pas, tant à cause de la trop grande fréquence de Z, qui représenterait *q*, que parce que *q* est toujours suivi de *u* et d'une voyelle, ce qui n'a évidemment pas lieu dans les quatrième et septième mots, où Z est suivi d'une seule lettre: nous ne pouvons donc traduire ZSJ que par *une*.

Relevons les lettres trouvées, tant pour les vérifier que pour continuer nos recherches, si elles semblent bonnes :

1	2	3	4	5	6	7
JQQJ	JXY	UFWYNJ	UTZW	ZSJ	IJXYNSFYNTS	NSHTSSZJ
e l l e	*e s t*	*. . . t . e*	*. . u .*	*une*	*. e s t . n . t . . n*	*. n . . n n u e*

Les solutions trouvées étant satisfaisantes, cherchons la valeur de N; par sa fréquence et la position qu'elle occupe, au sixième mot, entre un *t* et un *n*, nous sommes forcés d'y reconnaître une voyelle; *e* et *u* étant déterminés, il ne reste que *a*, *i*, *o*; ni *a* ni *o* ne sont admissibles, dans le troisième mot, entre *t* et *e*, donc N = *i*.

La position de F, au sixième mot, entre *n* et *t* indique une

voyelle, probablement un *a*, et celle de T, au septième mot, détermine la cinquième voyelle. T = *o*. Il vient donc :

1	2	3	4	5	6	7
JQQJ	JXY	UFWYNJ	UTZW	ZSJ	IJXYNSFYNTS	NSHTSSZJ
elle	*est*	*.a.tie*	*.ou.*	*une*	*.estination*	*in.onnue*

et on lit sans difficulté : *elle est partie pour une destination inconnue*.

Si, après avoir déterminé J = *e* et Q = *l*, nous avions compté les intervalles qui, dans l'alphabet normal, séparent E de J et L de Q, nous aurions reconnu qu'on avait employé la méthode de Jules César et chiffré avec le sous-alphabet de Vigenère commençant par F, ou, ce qui revient au même, avec deux bandes alphabétiques normales et la clé F (système de Vigenère).

Lorsque les mots du cryptogramme *ne sont pas séparés*, la méthode qui précède est difficilement applicable et le déchiffrement est plus laborieux.

Il faut surtout, dans ce cas, étudier la *physionomie* des lettres pour en déduire leur nature d'abord et ensuite leur valeur. Le colossal travail de M. Valério nous fournit de précieux renseignements à ce sujet. Nous allons appliquer ses ingénieux procédés à un cryptogramme qui, sans eux, serait absolument indéchiffrable.

Mais auparavant, nous donnons, ci-après, un tableau, déduit du travail de M. Valério et précisant bien la physionomie des diverses lettres et leurs rapports les unes avec les autres.

Rappelons d'abord que la proportion des voyelles et des consonnes varie peu : sur 100 lettres, on compte en moyenne 44,5 voyelles ; la variation est de deux en plus ou en moins. Il en résulte que l'intervalle qui sépare deux voyelles est de 100 : 44.5 ou 2,25 environ.

Les relations entre les voyelles et les consonnes sont assez stables ; elles sont résumées dans le tableau suivant :

O	U	I	A	E	Voy.	Cons.		Cons.	Voy.	E	A	I	U	O
7,4	3,4	3,8	3,8	5,2	23,6	76,4	Voy. 100	72,2	23,8	5,6	2,6	5,6	8 »	2 »
4,9	9,9	13 »	9 »	21,9	58,7	41,3	Cons. 100	29,6	70,4	26,6	14,9	6.9	8,8	13,2
....	....	....	....	....	....	....	....	....	....	....	....	....	....	....
5,4	8,5	11,1	8 »	18,4	51,4	48,6	100	39,3	60,7	22,2	12.3	6,7	8,5	11 »

Il ressort de ce tableau que, sur 100 voyelles, 76 sont précédées et suivies de consonnes, tandis que, sur 100 consonnes,

58,7 sont précédées de voyelles et 70,4 en sont suivies; que les voyelles qui précèdent les consonnes sont surtout E (21,9) et I (13 fois), et que celles qui les suivent le plus généralement sont E (26.6), A (14,9) et O (13,2).

Le tableau ci-dessous fournit les mêmes renseignements pour chaque lettre en particulier :

Lettres précédentes.								*Lettres suivantes.*						
O	U	I	A	E	Voy.	Cons.		Cons.	Voy.	E	A	I	U	O
»	3	7	»	4	14	86	E	87	13	4	3	1	5	»
»	7	2	1	7	17	83	A	83	17	»	1	9	7	»
10	7	»	10	2	29	71	I	72	28	16	2	»	»	10
27	»	»	8	13	48	52	U	77	23	8	7	8	»	»
»	»	10	»	»	10	90	O	62	38	»	»	10	28	»
21	10	8	13	30	82	18	N	62	38	19	7	2	2	8
10	14	7	18	19	68	32	R	42	58	24	10	10	3	11
7	9	8	3	41	68	32	S	51	49	18	5	12	8	6
1	8	17	10	17	53	47	T	49	51	20	5	17	4	5
1	3	10	12	22	48	52	L	22	78	44	17	7	5	5
1	1	6	1	32	41	59	D	7	93	47	19	12	12	3
6	11	2	7	23	49	51	C	25	75	20	15	2	11	27
13	9	7	9	43	81	19	M	19	81	41	7	18	2	13
2	15	»	19	28	64	36	P	31	69	19	15	2	7	26
4	19	7	26	22	78	22	V	4	96	33	26	15	»	22
»	16	5	5	32	58	42	F	26	74	16	21	5	»	32
7	7	»	22	»	36	64	B	36	64	14	29	7	»	14
»	»	37	18	27	82	18	G	53	47	37	»	10	»	»
»	»	9	9	9	27	73	Q	»	100	»	»	»	100	»
»	»	»	»	25	25	75	H	»	100	75	12	»	13	»
»	25	75	»	»	100	»	X	50	50	38	»	12	»	»
»	40	»	»	20	60	40	J	»	100	40	»	»	»	60
20	»	»	»	»	20	80	Y	60	40	»	20	»	»	20
»	»	50	»	25	75	25	Z	25	75	»	75	»	»	»

Les chiffres ci-dessus représentent des centièmes; ainsi 100 E sont précédés de 86 et suivis de 87 consonnes; 100 N sont précédés de 82 voyelles, savoir : 30 E, 13 A, 8 I, 10 U et 21 O, et suivis de 38 voyelles, qui se décomposent en : 19 E, 7 A, 2 I, 2 U et 8 O.

Proposons-nous maintenant de déchiffrer le cryptogramme :

VPKCWBUIKJPDUGNUGIWIJAXJKPXWVGXCEJIW

Le compte de fréquence, c'est-à-dire le nombre des répétitions de chaque lettre ne fait pas ressortir l'*e*; trois lettres sont employées *quatre* fois, 5 le sont *trois* fois, 2 *deux* fois et 5 ne figurent qu'*une* fois.

Cherchons donc les *relations* de chaque lettre répétée.

$$\left.\begin{matrix}C\\I\\X\\I\end{matrix}\right\}W\left\{\begin{matrix}B\\I\\V\\\text{-o-}\end{matrix}\right.\quad\left.\begin{matrix}U\\G\\W\\J\end{matrix}\right\}I\left\{\begin{matrix}K\\W\\J\\W\end{matrix}\right.\quad\left.\begin{matrix}K\\I\\X\\E\end{matrix}\right\}J\left\{\begin{matrix}P\\A\\K\\I\end{matrix}\right.\quad\left.\begin{matrix}V\\J\\K\end{matrix}\right\}P\left\{\begin{matrix}K\\D\\X\end{matrix}\right.\quad\left.\begin{matrix}B\\D\\N\end{matrix}\right\}U\left\{\begin{matrix}I\\G\\G\end{matrix}\right.$$

$$\left.\begin{matrix}U\\U\\V\end{matrix}\right\}G\left\{\begin{matrix}N\\I\\X\end{matrix}\right.\quad\left.\begin{matrix}A\\P\\G\end{matrix}\right\}X\left\{\begin{matrix}J\\W\\E\end{matrix}\right.\quad\left.\begin{matrix}P\\I\\J\end{matrix}\right\}K\left\{\begin{matrix}C\\J\\P\end{matrix}\right.\quad\left.\begin{matrix}K\\X\end{matrix}\right\}C\left\{\begin{matrix}W\\E\end{matrix}\right.\quad\left.\begin{matrix}\text{-o-}\\W\end{matrix}\right\}V\left\{\begin{matrix}P\\G\end{matrix}\right.$$

D'après les tableaux de M. Valério (1), nous savons que la lettre *e* peut précéder ou suivre presque toutes les consonnes; elle admet donc peu les répétitions et nous ne pouvons pas attribuer la valeur *e* à W, à cause de ses relations multiples avec I; nous rejetons I pour la même raison, ainsi que U, G, et K. Des trois lettres J, P, X, qui semblent admissibles, nous donnons la préférence à la première à cause de sa plus grande fréquence et nous posons : J = *e*.

Reprenant le compte de fréquence, nous inscrivons au-dessus de chaque lettre le nombre de fois que cette lettre est précédée de *e* et au-dessous le nombre de fois qu'elle en est suivie :

$$\overset{1}{\underset{1}{4W}},\ \overset{1}{4I},\ 4J,\ 3P,\ 3U,\ 3G,\ \underset{1}{3X},\ \overset{1}{\underset{1}{3K}},\ 2C,\ 2V,\ B,\ D,\ \overset{1}{A},\ \underset{1}{E},\ N.$$

Les lettres U et G, qui n'ont aucune relation avec *e*, sont probablement des voyelles, admettons-les comme telles et pointons-les sur le cryptogramme :

VPKCWBUIKJPDUGNUGIWIJAXJKPXWVGXCEJIW
. *e* . . . . *e* *e* . *e*

Cherchons les deux voyelles inconnues et d'abord déterminons leur fréquence. La proportion normale des voyelles étant de 44,5 pour cent lettres, sera de $36 \times \frac{44,5}{100}$ pour nos trente-six lettres. Les trois voyelles connues : J = 4, U = 3 et G = 3, donnant 10 au total ; les deux inconnues auront donc une fréquence probable de 16 — 10 = 6, soit 4 ou 3 pour l'une et 2 ou 3 pour l'autre.

D'autre part, les six lettres, VPKCWB, formant le début du cryptogramme, doivent contenir une et probablement deux

(1) *Cryptographie*, pages 13 et 61.

voyelles ; le groupe de cinq lettres KPXWV, qui se trouve vers la fin, doit renfermer, au moins, une voyelle.

Des sept lettres contenues dans ces deux groupes, nous devons rejeter K à cause de ses relations avec *e* et B qui n'est employé qu'une fois et qui, en outre, précède immédiatement une voyelle. La lettre V figure deux fois, la première comme initiale et, à la seconde, elle précède immédiatement une voyelle ; elle présente le caractère de *l* ou de *d* ; rejetons-la.

Restent W, P, X, C ; malgré ses relations avec I, W peut être voyelle, ainsi que P, X et C. Pour déterminer la nature de ces lettres, nous aurons recours au calcul des intervalles qui séparent chacune de ces lettres des voyelles connues. Il est évident, en effet, que plus est grand l'intervalle existant entre les voyelles connues, plus il y a de chances pour qu'on y rencontre de nouvelles voyelles.

Les quatre intervalles où figure W sont respectivement de 6, 3, 5 et 2 lettres, total 16 ; intervalle moyen 16/4 = 4 ; P figure dans trois intervalles de 6, 2, 5 : moyenne 13/3 = 4.33 ; les intervalles de X sont 2, 5, 3 : moyenne 10,3 = 3,33 ; ceux de C sont de 6 et 3 lettres et leur moyenne de 9/2 = 4,5.

Les intervalles moyens de P et de C étant les plus étendus, nous admettrons ces deux lettres comme voyelles.

Ayant déterminé la *nature* des lettres ou, comme le dit M. Valério, opéré la *séparation des voyelles*, il reste à trouver leurs valeurs.

Les voyelles U, G, qui s'associent deux fois pour former la même diphtongue, ne peuvent, d'après le tableau précédent, être que *o*, *u* ; d'après le même tableau, nous sommes amenés à voir *e*, *a* dans le bigramme JP

Les voyelles seront donc : J = *e*, U = *o*, G = *u*, P = *a*, C = *i*.

Reportons-les sous les lettres du cryptogramme :

VPKCWBUIKJPDUGNUGIWIJAXJKPXWVGXCEJIW
. *a* . *i* . . . *o* . . *ea* . *ou* . *ou* . . . *e* . . *e* . *a* . . . . *u* . *i* . *e* . .

Cherchons maintenant les consonnes.

Ce qui frappe le plus le regard, c'est la diphtongue *ou* répétée à une lettre d'intervalle. Peu de mots français présentent cette particularité. D'abord, par suite de la non similitude des lettres D et N, nous ne pouvons admettre les mots : *joujou, coucou, tout, ou*... ; les mots : *douloureux, roucouler, soucoupe, Toulouse*... doivent être repoussés, ainsi que *nous* et *vous* suivis d'un verbe commençant par *ou*, tel que *oublier, ourdir*, à cause de l'éloignement, dans le texte, de la voyelle qui suit le deuxième *ou*. Un seul mot semble pouvoir traduire : D *ou* N *ou* IW, c'est *toujours*, ce qui nous donne quatre nouvelles lettres que nous inscrivons sous le cryptogramme.

V, qui commence la phrase et précède partout une voyelle, offre les caractères de *l*; donnons-lui cette valeur.

Restent deux lettres fréquentes : K et X, probablement *n* et *d*, toutes les autres lettres fréquentes étant déjà déterminées. D'après le tableau de la page 152, ce n'est qu'exceptionnellement que *d* précède une consonne et, en tous cas, il ne peut entrer dans la combinaison $\frac{\text{PXWV}}{a\ .\ s\ l}$ où, au contraire *n* semble indiqué; faisons donc X = *n*, ce qui semble entrainer K = *d* : $\frac{\text{KPXW}}{d\ a\ n\ s}$.

Les trois lettres qui manquent encore : B, A, E, n'empêchent pas de lire couramment le vers de Lafontaine :

La discorde a toujours régné dans l'univers.

Lorsqu'un cryptogramme a été chiffré avec une clé polylittérale, c'est-à-dire avec plusieurs alphabets, il faut, avant d'essayer de découvrir la valeur des chiffres, commencer par déterminer le nombre des alphabets employés pour arriver à leur séparation.

Pour obtenir ce résultat qui, pendant longtemps a semblé chimérique, M. Kerckhoffs a formulé les règles suivantes (1) :

« 1° Dans tout texte chiffré, deux polygrammes semblables » sont le produit de deux groupes de lettres semblables crypto- » graphiées avec les mêmes alphabets ;

» 2° Le nombre des chiffres compris dans l'intervalle des » deux polygrammes est un multiple du nombre des lettres de » la clé. »

Dans ces phrases, il faut entendre par *polygrammes semblables*, non des lettres simplement juxtaposées, mais des *lettres semblables semblablement espacées*, ainsi, dans le cryptogramme suivant :

GANMXIZZAJEEBQCAYXVBCPTWIKMGZTCSLDOAOCXWM

DJUCZLMEPAYHCIPDSPJLBJZNFI

les bigrammes semblables sont non seulement AY, mais encore AB, CL et CM, qui suffiront à déterminer le nombre des alphabets. Quant au déchiffrement, il sera bien difficile, sinon impossible, vu le peu de lettres de chaque alphabet. — (On a employé le chiffre de Vigenère, avec la clé : VALERIO).

Nous arrêterons là nos notions sur le déchiffrement. Les personnes désireuses de se livrer à cette étude trouveront des renseignements plus complets dans les travaux, que nous avons maintes fois cités, de MM. Kerckhoffs, de Viaris, Valério, etc.

Rappelons, avec ce dernier cryptologue, que l'étude des procédés d'investigation peut seule permettre d'établir des chiffres

(1) *Cryptographie militaire*, page 36.

qui soient soustraits à leur action et empêcher de bons esprits de se faire illusion sur la valeur de systèmes dont la lecture n'est qu'un jeu puéril. (*Cryptographie*, 1893, page 228).

Insistons encore sur un passage de la deuxième partie de son ouvrage. (*Cryptographie*, 1896, page 3) :

« La répétition est pour le déchiffreur le moyen de contrôle ; » c'est aussi le moyen de recherche. Plus les répétitions sont » clairsemées, *plus ardue* sera sa tâche. »

Nous n'avons pas parlé des procédés de déchiffrement applicables aux méthodes polygrammatiques, aucun travail sur ce sujet n'étant venu à notre connaissance et l'auteur s'étant efforcé d'éliminer tout ce qui pouvait fournir des indices quelconques au déchiffreur. Il a cependant reconnu que la possession d'un cryptogramme établi à l'aide d'un alphabet à 2 ou 3 chiffres et de sa traduction en clair, jointe à la connaissance du groupement, permet de reconstituer l'alphabet employé. On peut s'en convaincre en résolvant le problème proposé à la page 56 de la *Cryptographie nouvelle*, sachant que ce cryptogramme a été chiffré en groupant, au premier tour, par 5 et 4 alternativement et, au deuxième tour, par 7 uniformément.



TABLE DES MATIÈRES

TROISIÈME PARTIE

SUBSTITUTION COMPLEXE

QUATRIEME PARTIE

PROCÉDÉS AUXILIAIRES DE CHIFFREMENT

CINQUIÈME PARTIE

MÉTHODES DIVERSES

SIXIÈME PARTIE

APPAREILS CRYPTOGRAPHIQUES

Pages

SEPTIÈME PARTIE

CRYPTOGRAPHIE MILITAIRE

HUITIÈME PARTIE

DÉCHIFFREMENT



814. — Paris. — Imp. P. DUBREUIL, 18, rue Clauzel. Téléph. 108-61.

